Elementa doctrinae Residuorum

A

Caput primum

1.

Definitiones. Si numerus aliquis, quem moduli nomine denotabimus, duorum numerorum differentiam metitur, hi secundum illum congrui dicentur, sin minus, incongrui. Priori casu alteruter numerorum alterius residuum vocatur, posteriori non-residuum. Ita numeri 32, 11 congrui dicentur secundum modulum 7, quippe quorum differentia 21 per 7 dividitur; et sub eadem restrictione tam 11 ipsius 32, quam 32 ipsius 11 residuum appellabitur. Ceterum hic statim monere debemus, has notiones de numeris tantum integris valere, fractos penitus excludi. Ad negativos vero aeque ac ad positivos patent: quare etiam −19 & +1 secundum 5 congrui recte dicentur.

2.

Vulgo residui denominatio in duobus casibus adhibetur a se quidem diuersis sed qui ambo in nostra definitione continentur; scilicet in subtractione, vbi a numero numerus semel tantum, et in diuisione vbi a positiuo numerus toties subductus est quoties licuit priusquam ad negatiuum perueniatur. At in disquisitionibus generalioribus vocem significatione generaliori accipere non dubitauimus, praesertim quum haud facile vlla inde ambiguitas oriri possit.

3.

Omnes numeri, qui numero dato a secundum modulum m sunt congrui, sub hac formula comprehenduntur $a \pm km$, in qua k ~~numerum~~ valorem quemcunque integrum obtinere potest: sed ista formula eiusmodi tantum suppeditat proprietates numerorum congruorum, quales tales sine negotio intuitiue cognosci possunt: de qua re iam in praefatione sententiam diximus. —

Maiorem utilitatem afferet ad calculos contrahendos numeros congruos signo denotare: ad quod ob insignem inter eos et quantitates aequales analogiam*) hoc utemur $\equiv$, modulo quando ad ambiguitatem euitandam necessarium videbitur clausulis apposito. Exempla §. 1. igitur tali modo exhibentur $32 \equiv 11$ (mod. 7); $-19 \equiv +1$ (mod. 5),

4

Numeri dati secundum modulum datum residua progressionem constituunt ~~utr~~ arithmeticam utrinque infinitam, cuius terminorum contiguorum differentia modulo est aequalis. Quodsi 0 inter ea occurrat, hoc erit ~~omnium~~ magnitudine minimum: utrumque contiguum modulo aequale, cetera maiora. Sin secus, bina residua contigua signis contrariis affecta, modulo singula minora erunt, cetera cuncta

*) Propter magnam hanc analogiam, Dm. Le Gendre in commentatione quam infra saepius laudabimus per signum ipsum aequalitatis (=) id exprimit quod ~~proprie~~ a nostris numeris congruis proprie non differt.

maiora. Haec duo residua minima sine respectu signorum coniuncta modulum producent; quare nisi inter se sint aequalia, alterum moduli dimidio maius, alterum minus esse debebit. Ex his colligitur cuiuis numero congruum inueniri posse modulo minorem, vnicum, scilicet quando est cifra, alias duplicem. Talia residua κατ' ἐξοχὴν residua minima appellabimus, posteriori casu residuum minimum positiuum a negatiuo distinguentes. Residuum absolute minimum * istud erit, quod moduli dimidium non superat, quale itaque semper datur, imo adeo duplex, quando forte huic dimidio ipsi aequale euadit: quod tamen quoties modulus habetur impar fieri nequit.

5.

Ne quis in principiis haereat exempla quaedam adicimus. Sit numerus datus −17, modulus 5, habebimus progressionem residuorum ... −22, −17, −12, −7, −2, +3, +8 ..... Hic itaque −2 erit residuum ~~ab~~ minimum negatiuum simulque absolute minimum, +3 residuum minimum positiuum. Sit datus +15 prodibit series numerorum huic congruorum secundum 7,

$\ldots +22, +15, +8, +1, -6, -13 \ldots$ ubi, minimus positivus ac simul absolute minimus $+1$; minimus negativus -6. 5

Simili modo numerus $+3$ secundum modulum 6 sibi ipse est congruus minimus positivus, -3 minimus negativus, nihilque interest quemnam assumamus quando de absolute minimo quaeritur.

6.

His notionibus constitutis progredimur ad ~~primas~~ eas numerorum congruorum proprietates enumerandas quae quasi prima fronte se offerunt quibusque reliquam huius capitis partem destinavimus. Ex eo quod omnia numeri dati residua in eadem progressione ~~[illegible]~~ continentur confestim fluunt sequentia:

Si qui numeri eidem numero secundum modulum eundem congrui sunt, inter se erunt congrui secundum eundem modulum.

Quum haec moduli identitas et in sequentibus locum habeat taediosam repetitionem omittimus.

Numeri ~~[illegible]~~ congrui eadem habent residua minima et vicissim

Numeri qui eadem dant residua minima congrui erunt.

Ex. $109 \equiv -34$ (mod. 13); $109 \equiv 70$; ergo $70 \equiv -34$. Cuiusvis horum numerorum residua minima sunt $+5, -8$.

7.

Si habeantur quotcunque numeri a, b, c &c, ac totidem alii α, β, γ &c. illis singuli singulis congrui, $a \equiv \alpha$, $b \equiv \beta$, $c \equiv \gamma$ secundum modulum quemcunque, erit $a + b + c +$ &c. $\equiv \alpha + \beta + \gamma +$ &c.

Ex. 23, -15, 38 sunt congrui his 1, -4, -6 secundum modulum 11, ergo $46 \equiv -9$.

Demonstrationem ob facilitatem non addo. Posset ea etiam simili modo adstrui ut in multiplicatione statim docebimus

8

Si secundum modulum quemcunque $a \equiv \alpha$ et $b \equiv \beta$ erit et $a - b \equiv \alpha - \beta$.

Ex. $30 \equiv 2$, $14 \equiv 0$ (mod. 7); ergo. $16 \equiv 2$.

9

Si $a \equiv \alpha$ erit quoque $ka \equiv k\alpha$ unde etiam ob factorum permutationem permissam $ak \equiv \alpha k$

Si k est numerus positivus, hoc est tantum casus singularis propositionis §. 7., quando ~~omnes ibi~~ utrinque ibi omnes numeri aequales ponuntur. Quodsi esset negativum puta $-p$, atque adeo p positivum, erit $pa \equiv p\alpha$ ideoque $-pa \equiv -p\alpha$ sive $ka \equiv k\alpha$.

Ex. $17 \equiv -1$ (mod. 9) ergo $7.17 \equiv 119 \equiv -7$.

Cor. Si igitur $a \equiv 0$ seu per modulum divisibile erit et $ka \equiv 0$.

10.

Si $a \equiv \alpha$, $b \equiv \beta$, erit quoque $ab \equiv \alpha\beta$.

Scilicet ex § praec. erit $ab \equiv a\beta$; ~~$\alpha\beta$~~ et $a\beta \equiv \alpha\beta$, ac proin ex 6, $ab \equiv \alpha\beta$.

Ex. $19 \equiv 3$; $10 \equiv 2$ (mod. 8) ergo $190 \equiv 6$.

11.

Si habeantur quotcunque numeri a, b, c &c. ac totidem alii α, β, γ &c. illis singuli singulis congrui, erit productum ex illis congruum producto ex his $abc \ldots \equiv \alpha\beta\gamma$.

Ex praec. iam habemus $ab \equiv \alpha\beta$, itaque ex eodem fonte $abc \equiv \alpha\beta\gamma$, et eodem modo quotcunque alii factores continuo adiungi possunt.

Ex. $7.5.8\ (= 280) \equiv 1.2.2\ (= 4)$ (mod. 3). $+1.2.2$

12.

Omnibus utrinque numeris § praec. positis aequalibus prodit sequens theorema

Si $a \equiv \alpha$ et k numerus integer positivus erit $a^k \equiv \alpha^k$.

Ex. $10 \equiv 1$ (mod. 9) itaque omnes denarii potestates, unitati erunt congrui secundum hunc modulum.

Secundum modulum 11, $10 \equiv -1$ itaque $10^{2k} \equiv +1$, $10^{2k+1} \equiv -1$.

13.

Functio ~~Expressio~~ quaecunque variabilis unius algebraica rationalis quae nullam fractionem involuit, si in ea variabili valores congrui tribuantur, valores congruos adipiscetur.

Huiusmodi ~~f~~ functio talem formam habebit $ax^m + bx^n + cx^p + \&c.$ ubi $m, n, p \ldots$ sunt integri positivi. in qua si pro x valores congrui f, g, substituantur erit

$$af^m + bf^n + cf^p + \&c \equiv ag^m + bg^n + cg^p + \&c.$$

Veritas huius propositionis ex combinatione §§ 12, 11, 7 facillime evincitur

Caput secundum.

De residuis functionum primi gradus.

17.

Theorema. Productum e duobus numeris dato numero primo minoribus per hunc primum non dividitur.

Sit p primus et $a < p$ nego fieri posse ut sit $b < p$ et $ab \equiv 0$ mod. p. (Numeri hi omnes tamquam positivi spectantur, cifra excludintur)

Demonstr. Si negas assumamus dari tamen numeros $b, c, d \ldots$ omnes $< p$ et esse $ab, ac, ad \ldots \equiv 0$ (mod. p). Sit b omnium minimus ita ut infra ipsum nulli dentur illa proprietate praediti. Primo statim patet b esse non posse $= 1$ quia per hyp. $1.a < p$ per p nequit dividi. Quum igitur $b > 1$ et p primus, b ipsum p non metietur ac proin p intra duo ipsius b multipla proxima cadet, quorum alterum $mb > p$, alterum $(m-1)b < p$. Est ergo $mb - p (= \mathfrak{b}) < b$. Iam quia supponimus esse $ab \equiv 0$ (mod. p) erit etiam $amb \equiv 0$ (§9) et propter $mb \equiv \mathfrak{b}$

etiam $a\mathfrak{b} \equiv 0$. Igitur ~~et~~ $\mathfrak{b}$ quoque illam numerorum $b, c, d \ldots$ proprietatem habet: at b per hyp. est minimus Q.E.A.

18.

Si nec a nec b per numerum primum p diuiditur etiam ab per p non diuidetur.

Dem. Sint numerorum a, b secundum modulum p residua minima positiua $\alpha, \mathfrak{b}$ quorum neuter erit 0 per hyp. Ergo $ab \equiv \alpha\mathfrak{b}$ (mod. p) ac si esset $ab \equiv 0$ foret etiam $\alpha\mathfrak{b} \equiv 0$, quod per theor. praec. fieri nequit.

Theorema hoc sub quo praecedens continetur iam ab Euclide demonstratum habetur VII.32 quem adeant qui methodos aliquantum diuersas comparare student: in libris nostris arithmeticis etiam optimis plerumque desideratur. Nos demonstrationem eo minus omittendam duximus, quia methodo hic adhibita ad quaestiones in hoc genere intricatissimas enodandas eximio successu utemur. Quare eius indolem lectoribus commendamus antequam illa adeant probe perpendendam.

sua numquam probabiliter relationes subministraturas esse ob concinnitatem, geometrarum laboribus satis dignas. — Functiones istae algebraicae tamen non sunt unicae de quibus huiusmodi disquisitiones instituti possint: excluduntur duntaxat eae quae ad quantitates fractas deducunt: quare etiam expressiones exponentiales, vt ex gr. a^x, summae potestatum radicum aequationis algebraicae &c &c huc trahendae erunt.

16.

Theorematibus in hoc capite contentis complura quae in libris arithmeticis doceri solent innituntur, ex. gr. regulae pro exploranda diuisibilitate numeri propositi per 9, 11 &c. Secundum modulum 9 omnes ~~ep~~ numeri 10 potestates vnitati congrui sunt: quamobrem, quoad residua minima secundum hunc modulum, perinde est vtrum in numero decadice expresso ad locum quem singulae figurae occupant respiciatur necne. Ex. gr. numerus $3825 \equiv 3+8+2+5$ quia $3000 \equiv 3$; $800 \equiv 8$ &c. (mod. 9). Ergo 3825 per 9 diuisum idem residuum minimum relinquit quod 18, scilicet nihil cifram. Idem de modulo 3 tenendum. Quum secundum modulum 11 omnes denarii potestates exponenti pari congruae sint vnitati positiue, impari vero exponenti, negatiue sumtae, figurae numeri propositi locum ~~imparem~~ parem occupantes (a dextra ad laeuam) signo negatiue afficiendae atque dein cum ceteris positiue sumtis iungendae sunt vt numero dato congruus prodeat.

Ex eodem fonte petuntur Criteria ad quae operationes arithmeticae examinantur. Scilicet numerorum additorum, subductorum, multiplicatorum siue ad potestatem euectorum residua minima assumuntur secundum modulum arbitrarium (vulgo 9 vel 11, quia hi vt modo ostendimus in nostro systemate dyadico ad numeros congruos inueniendos perquam adaptati sunt) atque haec eodem modo quo numeri propositi tractantur: si quae vtrinque proueniunt sint incongrua, menda calculo inesse debet.

Sed haec tam trita sunt ac facilia vt diutius iis immorantes lectorum patientia abuti vereamur.

Ex. sit $a = 3$ et $p = 7$. Habebimus seriem residuorum 17

0, 3, 6, 2, 5, 1, 4. C.

Si negas ponamus ex multiplicatoribus diversis m, n quorum prior sit maior provenire residua aequalia, seu esse $ma \equiv na$ (mod. p). Ergo $(m-n)a \equiv 0$ et ob a ad p primum, (ex §21) erit $m-n$ per p divisibilis. At $m < p$, ergo $m-n < p$ et ob id ipsum per p non divisibilis. Q.E.A.

Quum igitur multitudo illorum productorum a $0.a$ usque ad $(p-1)a$ sit aequalis p habebimus p residua diversa omnia numero p minora. Totidem autem dantur numeri infra p a 0 usque ad $p-1$, quorum igitur nullus in illa serie deesse potest.

$\frac{\alpha^6 y'^3}{d}$

$\frac{1+y'y'^3}{y''y''}$

$\frac{1+\alpha\alpha y'y'^3}{\alpha y''\alpha y''}$

$\frac{(1+y'y')^3}{y''y''} = r$

$y = mx^n$ $\quad \frac{1+m^2n^2x^{2n-2}}{m^2n^2(n-1)^2x}$ $\quad r = \frac{s'^3}{y''}$ $\quad aa = (y+b)^2(y'$ $\quad aa = (y+b)^2(1+y'y')$

$2ydy = a-2x$

$ydy = -xdx$

$yddy + dy^2 = -dx^2$

23.

Formula $ax+b$, (in qua a, b denotant numeros datos, x numerum arbitrarium seu variabilem) secundum modulum primum p ipsum a non metientem cuivis numero dato congrua fieri potest.

$(y+b)^2 + (x+c)^2 = aa$

$\cancel{0 = (y+b)dy + (x+c)dx}$

$0 = (y+b)y' + x + c$

$0 = y'y' + (y+b)y'' + 1$

Sit numerus cui congrua fieri debet A et quaeratur

$\frac{(y'y'+1)^2}{y''y''}$

residuum minimum positiuum differentiae $A - b$, secundum mod. p, quod sit α. Ex § praec. semper datur valor ipsius x, $< p$, ~~qui~~ ut residuum minimum producti ax sit $= \alpha$. Erit igitur pro hoc valore $ax \equiv \alpha \equiv A - b$, siue $ax + b \equiv A$. Q.E.F.

Expressionem duas quantitates congruas exhibentem ad instar aequationum <u>congruentiam</u> vocabimus; quae si quantitatem incognitam inuoluat, <u>resolui</u> dicetur quando pro ea valor inuentus est qui congruentiae satisfaciat. Hinc intelligitur quid sit <u>congruentia resolubilis</u> et <u>congruentia irresolubilis</u>. Talis congruentia $ax + b \equiv c$ itaque semper resolutionem admittet quoties modulus est primus et ipsum a non metitur. ~~Pat~~ Ceterum patet si ξ est valor idoneus pro x, etiam $\xi \pm mp$ satisfacere, siue omnes numeros, ipsi ξ secundum p congruos.

24.

<u>Si congruentiae $ax + b \equiv c$ (mod. p. prim.‡) satisfaciunt $x = \xi$ et $x = \xi'$ erit $\xi' \equiv \xi$ (mod. p).</u>

‡ <u>a non metiens</u>

Quia $a\xi + b \equiv c$ et $a\xi' + b \equiv c$ erit $a(\xi' - \xi) \equiv 0$ (§ 8), ergo $\xi' - \xi \equiv 0$. (§ 21) siue $\xi' \equiv \xi$
Q.E.D.

Quum resolutiones per valores ipsius x congruos per se sint obuiae atque hoc respectu numeri congrui tamquam aequiualentes spectari possint, tales congruentiae resolutiones pro vna eademque sunt habendae. Quoniam igitur congruentia nostra $ax+b\equiv c$ huiusmodi tantum resolutiones admittat, pronunciabimus vnico eam tantum modo esse resolubilem. Ex. gr. congruentia $6x+5\equiv 13 \pmod{11}$ per alios ipsius x valores resolui nequit nisi qui numero 5 secundum 11 sunt congrui. Secus sese habent congruentiae altiorum graduum, nec non et primi quoties modulus non est primus.

25.

Omnia quae §§ 22...24 docuimus aeque locum habent pro congruentia $ax+b\equiv c \pmod{z}$, quamquam z non sit primus, si modo nullum cum a habeat diuisorem communem: quod quia quiuis statim ~~sponte~~ nullo negotio intelliget, superfluum foret omnia hic pro illo casu repetere. Tales congruentia ergo semper resolui poterit et quidem unico modo, hac expressione ita vt modo definiuimus accepta.

26.

Postquam demonstrauimus congruentiam $ax+b\equiv c$

resolutionem dari, liceat pauca adiicere de methodo reuera illam inueniendi quamuis hic vt in re hoc tempore quidem notissima breues esse possumus. Primum obseruo omnium harum congruentiarum resolutionem pendere ab hac $ax \equiv \pm 1$, scilicet si huic satisfaciat $x = \xi$, satisfaciet congruentiae $ax + b \equiv c$, $x = \pm(c-b)\xi$. Sed congruentia $ax \equiv \pm 1$ ~~aequ~~ (mod. f) aequiualet aequationi indeterminatae $ax = fy \pm 1$ (~~inque~~ vbi a ~~#~~ ad f ~~#~~ supponitur esse primus) quam constat aut sponte resolui, scilicet quando altera quantitatum a, f est $= 1$, aut per substitutiones conuenientes repetitas ad talem semper reduci posse. ~~Si quis lectorum methodi huius sit ignarus~~ Quum in hoc opere propositum nobis sit res notas tantum attingere, sufficiet in eorum gratiam qui forte methodi huius sint ignari exemplum adiicere. Sit data aequatio indeterminata ... $83x = 16y \pm 1$. Diuidatur coefficiens maior 83 per minorem 16, et quum quotiens sit $\frac{5}{\pm}$, neglecto quod superest, faciamus $y = 5x + p$ quo valore substituto prodibit aequatio priori similis $3x = 16p \pm 1$. Iterum sumatur $x = 5p + q$ et erit $3q = p \pm 1$ quae aequatio quum coefficiens ipsius p, $= 1$ soluitur sumendo $q = 0$, hinc $p = \mp 1$, $x = \mp 5$, $y = \mp 26$. Congruentia $83x \equiv \pm 1$ (mod. 16) resoluitur itaque per $x = \mp 5$ aut per valores huic congruos $\mp 5 \pm 16n$.

27.

Ill. Euler huiusmodi aequationes indeterminatas primus generaliter resoluere docuit Comm. Petrop. VII. p. 46. ~~quem~~ ~~[illegible]~~ Si quis operationes ad hunc finem adhibendas attente perpendat facile inueniet, easdem esse quibus utimur ad maximam inter a et f mensuram explorandam, siue etiam ad fractiones inueniendas ab illa $\frac{a}{f}$ continue minus discrepantes. Quod eo minus mirum videri debet quum constet duas tales fractiones ~~huiusmodi~~ contiguas $\frac{m}{n}$ et $\frac{m'}{n'}$ eius esse indolis vt sit $mn' - m'n = \pm 1$, ex quo statim sequitur, inuenta fractione illam $\frac{a}{f}$ immediate praecedente, quae sit $\frac{y}{x}$ problema esse solutum fierique $ax = fy \pm 1$. ~~[illegible]~~ Hanc methodum explicauit Ill. La Grange (Mém. de l'Ac. de Berlin Année 1767 p. 175 *))

*) Inuestigationes in hac commentatione vt et in quibusdam subsequentibus contentae ~~inueniuntur~~ exstant etiam in Supplem. quae Ill. La Grange ad versionem gallicam Algebrae Euleri adiecit, quorumque anno praec. versionem germanicam a Dm. Kausler accepimus.

Progredimur ad congruentias $ax + b \equiv c$ in quibus a ad modulum non est primus. Ponamus igitur $a = kA$ et modulum $= kz$ ut sit A ad z primus. ~~Sit minimus valor ipsius x positivus~~ ~~a qui datur~~ ~~congruentiam soluens $= \alpha$, ceterique qui omnes modulo minores accipi possunt~~ ~~ordine suo~~ $\beta, \gamma, \delta \ldots x$. Erit itaque

$$kA\alpha + b \equiv c$$
$$kA\beta + b \equiv c \quad \&c.$$
$$kAx + b \equiv c$$

Hinc

$kA(\beta - \alpha) \equiv 0$ &c

$kA(x - \alpha) \equiv 0$ hinc

$\frac{kA(\beta - \alpha)}{kz}, \ldots \frac{kA(x - \alpha)}{kz}$ erunt numeri integri hinc $\beta - \alpha, \gamma - \alpha, \ldots x - \alpha$ per z diuiditur, quumque β, γ tanquam ~~continuo maiores assumantur poni oportet $\beta - \alpha = z$, $\gamma - \alpha = 2z \ldots$~~

Praeterea assumamus congruentiam esse reuera resolubilem ~~indeterminatam~~ eique satisfieri ponendo $x = \xi$. Patet tunc etiam satisfacere ~~[illegible]~~ $x = \xi \pm nz$ quando n numerum quemcunque integrum denotare potest. Sed dico

<u>in hac formula omnes ipsius x valores esse comprehensos.</u>

Quando enim etiam satisfacit $x = \xi'$ erit tum $kA\xi + b \equiv c$ tum $kA\xi' + b \equiv c$; unde $kA(\xi' - \xi) \equiv 0$. Ergo $kA(\xi' - \xi)$ per modulum kz diuiditur, siue $A(\xi' - \xi)$ per z

At A et z sunt inter se primi, proin ~~oportet~~ necessario ~~et~~ $\xi'-\xi$ debet esse multiplum ipsius z.

29.

Ex uno valore ipsius x, congruentiae $kAx+b\equiv c \pmod{kz}$ satisfaciente derivantur igitur omnes ceteri addendo aut subtrahendo z, $2z$, $3z$ &c. Sed quum kz = modulo post k additiones aut subtractiones valores prodibunt valores prioribus congrui qui igitur secundum principia nostra pro iisdem sunt habendi. Omnes ~~igitur~~ ergo valores diversi comprehenduntur in hac serie ξ, $\xi+z$, $\xi+2z$ .... $\xi+(k-1)z$ (signum ~~minus~~ negativum daret valores his ordine inverso aequivalentes.) Proinde multitudo omnium resolutionum diversarum aequalis est k.

30.

Supposuimus ~~datam aequatio~~ congruentiam resolvi posse, videamus nunc quomodo hoc sit diiudicandum valorque unus saltem ~~possit~~ explorandus. Quia $kAx+b\equiv c \pmod{kz}$ haec congruentia etiam pro modulo k valere debet; seu debet esse $b\equiv c \pmod{k}$ Quodsi hoc non eveniat congruentia illa certo resolvi nequit. Si vero ~~[illegible]~~ $c=b+mk$ congruentia nostra hanc induet formam $k(Ax-m)\equiv 0 \pmod{kz}$ cui satisfiet, si $Ax-m$ factum est per z divisibile seu per resolutionem huius congruentiae $Ax - m \equiv 0 \pmod{z}$ quae semper datur quia A ad z est primus. (§ 25)

31

Ex. Proposita sit congruentia $21x + 5 \equiv 32$ (mod. 30) Hic igitur maximus divisor numerorum 21 et 30 $= 3$ at quum secundum modulum 3 ~~congruentia~~ 5 et 32 non sint congrui, ~~etiam~~ illa congruentia resolvi nequit.

*) Attamen 27 divisibile per 3; praeterea $32 \equiv 5$ (M: 3) hinc quoque $21x + 5 - 32 = 3(7x - 9) \equiv 0$, tamen ponendo $x = 7$ erit $3(49 - 9) \equiv 0$ quoniam divisibile per 3·10.

Proponatur iterum $15x + 17 \equiv 12$ (mod. 20). Divisor maximus numeris 15 et 20 communis ~~8~~ hic est 5 secundum quem $17 \equiv 12$. Detur itaque congruentiae propositae haec forma $5(3x + 1) \equiv 0$ (mod 5.4). Quaeratur valor ipsius x huic congr. satisfaciens $3x + 1 \equiv 0$ (mod. 4) qui erit $x = 1$, ~~et~~ atque etiam congr. primariae satisfaciet. Ceteri valores ex 28 eliciuntur $x = 5, 9, 13, 17$

Si Chordae vibrationes cum in eodem plano fiant eruntne illae quae in eodem plano fiunt isochronae?

32.

Ex iis quae hactenus exposita sunt colligitur omnes congruentiae resolutiones sive sint aequivalentes sive non semper per congruentiam exhiberi posse. Scilicet ~~omnes~~ resolutiones huius congruentiae $ax + b \equiv c$ (mod. z) si a et z sunt primi inter se ita: $x \equiv \xi$ (mod. z); si vero a et z habeant divisorem communem maximum k et sit $z = kt$, hoc modo $x \equiv \xi$ (mod. t.). Hinc

Formula

facile monstrare possumus quomodo numerus inveniatur qui pluribus congruentiis simul satisfaciat. Ponamus ex prima harum congruentiarum sequi $x \equiv \alpha \pmod{A}$; ex secunda $x \equiv \beta \pmod{B}$. Si itaque quaeritur valor ipsius x qui utrique satisfaciat debet esse $By + C = x$ et $x \equiv \alpha \pmod{A}$ sive $By + C \equiv \alpha \pmod{A}$. Si haec congr. est impossibilis ~~quod~~ fieri nequit quod desiderabatur; ~~si autem~~ ~~si~~ Secus ~~exhibentur~~ ~~exhibeantur~~ omnes eius resolutiones ita exhiberi possunt $y \equiv v \pmod{t}$, ubi t erit maxim ~~mensura~~ divisor numerorum A et B†; hinc omnes valores ipsius x in hac ~~congruentia~~ forma comprehensi erunt:

| † sive hoc modo $y = v + nt$

~~$Bv + C \bmod t$~~ $x = Bv + Bnt + C$, ubi n numerum quemcunque integrum denotat, ceterae quantitates sunt data. Per congruentiam igitur x ita exprimitur $x \equiv Bv + C \pmod{Bt}$. Eodem modo procedendum erit si plures adhuc conditiones accedant quibus x satisfacere debet

33

Quoniam hoc problema per totum hunc librum saepissime occurret exemplo illustrare non erit inutile. Quaeritur expressio omnes valores ipsius x amplectens, qui simul his tribus congruentiis satisfaciant (1) .... $5x + 2 \equiv 0 \pmod{9}$;
(2) .... $6x + \overset{15}{\cancel{14}} \equiv 0 \pmod{21}$; (3) .... $3x + 3 \equiv 0 \pmod{4}$
Elicientur valores ipsius x ex (1) $x \equiv +5 \pmod{9}$;

ex (2) $x \equiv 1 \pmod{7}$; ex (3) $x \equiv 1 \pmod{4}$

Combinando valorem primum et secundum et statuendo $x = 9y + 5$. pervenimus ad hanc congruentiam: $9y + 5 \equiv 1 \pmod{7}$ cui satisfit sumendo $y \equiv 5 \pmod{7}$ hinc $x \equiv 50 \pmod{63}$ ~~hinc x ≡ ... (4)~~

Combinando iterum hunc valorem cum tertio et statuendo $x = 63z + 50$: habetur $63z + 50 \equiv 1 \pmod{4}$; ~~cui~~ hinc ~~satisfit per~~ $z \equiv 1 \pmod{4}$ et tandem $x \equiv 113 \pmod{252}$ quae expressio omnes valores tribus congruentiis datis satisfacientes amplectitur.

34.

Sufficiant haec de congruentiis primi gradus. Unum hoc adhuc monemus quod ~~plerumque~~ earum usus per totam hanc doctrinam est amplissimus, atque ideo ~~hanc etiam~~ lectoribus commendamus facilitatem eas tractandi sibi comparare ut compendia ad calculos contrahendos quae plurimum sese offerunt arripere possint. Sed de his docere non est nostri instituti, ~~neque et neque~~ atque haec non tam e regulis quam ex usu ediscuntur. — Sed antequam huic capiti finem imponamus propositiones quasdam adiiciemus quibus in sequentibus ~~[illegible]~~ ~~ad~~ utemur, sed quarum demonstrationes hic demum rigorose adornari possunt.

$$A(\Delta 1)^m + P(\Delta 1)^{m-1} + Q(\Delta 1)^{m-2} \ldots + Z \equiv 0$$
$$A(\Delta 2)^m + P(\Delta 2)^{m-1} + Q(\Delta 2)^{m-2} \ldots + Z \equiv 0$$
$$\vdots \qquad \vdots \qquad \vdots$$

In quibus $P, Q, R \ldots$ ab $A, B, C \ldots$ et a (1) dependebunt. Z autem erit $= A(1)^m + B(1)^{m-1} \ldots + N$ ut cuiuis attente genesin ponderanti sine negotio patebit. At prima congruentia dat $Z \equiv 0$ unde nostrae formulae hanc induent formam

$$(\Delta 1)\left(A(\Delta 1)^{m-1} + P(\Delta 1)^{m-2} + \ldots + Y\right) \equiv 0$$
$$(\Delta 2)\left(A(\Delta 2)^{m-1} + P(\Delta 2)^{m-2} + \ldots + Y\right) \equiv 0$$
$$\vdots \qquad \vdots$$

At $\Delta 1, \Delta 2 \ldots$ omnes sunt $< p$; igitur etiam id quod per eos multiplicatum est cifrae congruum esse debet. Itaque congruentia $At^{m-1} + Pt^{m-2} \ldots + Y$ resolvitur per $x = \Delta 1, \Delta 2, \Delta 3 \ldots \Delta m$ seu m diversis modis i.e. dantur etiam congruentiae gradus minoris quae m ~~gradus m non est maximus qui~~ theoremati nostro repugnat. Q.E.A.

38.

Congruentiae secundi gradus igitur duas tantum resolutiones diversas admittunt, tertii gradus tres, quarti quatuor & sic porro. Si coefficiens termini summi ~~maxim~~ A per p dividitur hunc omnino negligere possumus quia tunc $Ax^m \equiv 0$. Si modo unus coefficientium per p non dividatur igitur theorema nostrum ~~neq~~ etiam locum tenet. Sin autem omnes coefficientes

ad summum

sint per p divisibiles patet congruentiam esse identicam sine quidvis pro x substitui posse.

Theorema hoc primum ab ill. La Grange generaliter propositum et demonstratum (Mem. de l'Ac. de Berlin Année 1768 p. 192 atque iterum Nouv. Mem. de l'Ac. de Berlin Année p. . Extat etiam in dissert. ill. Le Gendre Recherches d'Analyse indeterminée Hist. de l'Ac. Roiale de Paris. 1785 p. Casum particularem congruentiae $x^m \equiv 1$ ~~[illegible]~~ cuius in capite sequente frequens usus erit primus exposuit ill. Euler in dissertatione Comm. Nov. Petrop. T. V. p. .

generaliter

~~quamquam et~~ genere hic casus a viro summo ~~generaliter demum~~ absolutus ~~est~~ est in commentatione Novorum Comm. T. XVIII inserta p. 99.

Demonstratio hic explicata est ea in quam incidi priusquam La Grangianam novissem a qua non multum discrepat. [Sed infra ~~libro~~ capite octavo ‡ aliam trademus multo simpliciorem et quae ~~sola~~ e principiis magis genuinis hausta esse videtur.] — Ceterum de modulis ~~comp~~ non primis seorsim

‡ ubi congruentias methodo ~~plane~~ prorsus singulari pertractabimus

agere supersedere possumus

Probl. Inuenire quot numeri dentur qui numero proposito N sint minores ad eumque primi.

Sol. 1.° Sit A primus, patet omnes numeros ab 1 usque ad $A-1$ ad N fore primos ideoque eorum multitudinem $= A-1$.

2°. Sit A dignitas numeri primi puta p^m; ~~patet~~ hinc omnes numeri per p diuisibiles ad p^m non erunt primi, ceteri erunt. Itaque ex $p^m - 1$ numeris excluduntur $p, 2p \ldots (p^{m-1}-1)p$ restant igitur $p^m - 1 - (p^{m-1}-1) = p^{m-1}(p-1)$.

3.° Ceteris casibus constat N semper compositum esse ex huiusmodi factoribus p^μ, q^ν &c p, q.. numeros primos diuersos denotantibus. Ad hunc igitur casum enodandum generalissime ponamus datum esse productum ab, in quo a et b inter se sunt primi sitque ~~num~~ multitudo numerorum ad hos respective primorum α et 6. Denotentur illi per $A, A', A'' \ldots$, hi per $B, B', B'' \ldots$ ~~qui om~~ quorum priores omnes erunt $< a$, posteriores $< b$. Numeri igitur omnes ad a primi infra ab in his seriebus ~~serie~~ exhibebuntur

$A, A', A'' \ldots, a+A, a+A', a+A'' \ldots 2a+2A, 2a+2A', 2a+2A''$,

$\ldots, \ldots,$ ~~$a+(b-1)$~~ $(b-1)a+A, (b-1)a+A', (b-1)a+A'' \ldots$

seu potius ita

$$\begin{array}{llll} A, & A+a, & A+2a \ldots & A+(b-1)a \\ A' & A'+a & A'+2a \ldots & A'+(b-1)a \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

ubi dabuntur α series horizontaliter positae quarum quaeuis b terminos continet. ~~[illegible]~~ $A+\alpha$, ...

At in serie $0, a, 2a \ldots (b-1)a$ unicus tantum datur terminus qui per b divisus residuum $B-A$, ~~suppeditat~~, unicus porro qui residuum $B'-A$, unicus qui $B''-A$ suppeditat &c... (§ 22, 25), sive in serie $A, A+a, A+2a \ldots A+(b-1)a$, unus terminus post divisionem per b dabit B, unus B', unus B''.... sed hi omnes ad b erunt ~~...~~ primi ceteri qui alium residuum praebent non erunt quare in prima serie erunt $\mathfrak{b}$ numeri ad b primi, sed methodo omnino huic simili idem de ceteris seriebus demonstratur. Quare inter omnes numeros ad a primos erunt $\alpha\mathfrak{b}$ ad b primi et quum ceteri ~~aut~~ cum alterö numerorum ~~a aut qu~~ a, b certe factorem habeant communem sequitur hoc theorema:

multitudo numerorum $< ab$, ad ab primorum erit $= \alpha\mathfrak{b}$.

Iam facillimum erit haec ad nostrum casum adaptare sit $A = p^\mu q^\nu r^\rho \ldots$ et erit ~~mul~~ numeri ad $p^\mu, q^\nu, r^\rho \ldots$ primi atque ~~et~~ ipsis $p^\mu, q^\nu, r^\rho \ldots$ respective minores $p^{\mu-1}(p-1)$; $q^{\nu-1}(q-1)$; $r^{\rho-1}(r-1) \ldots$ ideo primi ad $p^\mu q^\nu$ infra $p^\mu q^\nu$ ~~multitud.~~ dabuntur $p^{\mu-1} q^{\nu-1}(p-1)(q-1)$. Pro $p^\mu q^\nu r^\rho$ accedet adhuc factor $r^{\rho-1}(r-1)$, et sic porro. Q. E. I.

Ceterum haec formula aliquantulum concinnius exhibetur hoc modo $A \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r} \ldots$

36.

~~Formulam hanc [illegible] continuius [illegible]~~

~~hoc modo : $A \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r}$~~

Exempl. Sit $A = 60 = 2^2 . 3 . 5$. proin multitudo numerorum ad 60 primorum $< 60 = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 60 = 16$. Numeri hi sunt

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

Exstat hoc problema primum solutum ab ill. Euler in commentatione inscripta, Theoremata arithmetica noua methodo demonstrata Comm. nou. Acad. Petr. VIII. p. 74. Demonstratio postea repetita est in alia diss. Speculationes circa quasdam insignes proprietates numerorum. Acta Ac. Petr. VIII p. 18

37.

~~Vidimus omnes congruentias primi gradus in quibus numerus primus pro modulo assumitur unico tantum modo resolui posse; inuestigandum iam est quot modis diuersis aequationes altiorum graduum admittant~~

Theor. Si omnes resolutiones congruentiae $Ax^m + Bx^{m-1} + \ldots + M \equiv 0$ (mod. p, primus, qui A non metitur) qui per valores ipsius x secundum p congruos procedunt pro unica habeantur, plures quam m eius resolutiones diuersae dari nequeunt.

<u>Dem.</u> Si negas ponamus dari congruentias graduum respective $m, n, p \ldots$ in inf. quae plures quam $m, n, p \ldots$ resolutiones diversas admittant, sitque minimus gradus, m. ita ut omnes congruentiae inferiorum graduum duvesmodi ~~plures~~ resolutionum diversarum numerum maiorem eo ~~quam~~ qui ~~est~~ gradum ~~index~~ indicat non admittant. Talem restrictionem esse concedendam apparet ex eo quod ~~Nam~~ de aequationibus primi gradus theorema iam sit ~~est~~ demonstratum, ~~quare m certe non est 2~~. quare m ad minimum erit 2. Admittat igitur congruentia

$A x^m + B x^{m-1} \ldots + N \equiv 0 \pmod{p}$ saltem $m+1$ resolutiones $x = (1)$, $x = (2)$, $x = (3)$, $\ldots$ $x = (m+1)$ qui valores omnes modulo p minores accipi possunt. Sit minimus eorum (1).

~~Statim observo, pro casu quo p non est > m ne quaestionem quidem esse posse, quia tunc plures quam m valores diversi ne quidem fingi possunt sine respectu etiam resolubilitati congruentiae per se~~. Ad contrahendos calculos designo $(2)-(1)$ per $(\Delta 1)$; $(3)-(1)$ per $(\Delta 2)$ $\ldots$ $(m+1)-(1)$ per (Δm), ~~expressionemque illam $Ax^m + Bx^{m-1} \ldots$ per φx. Est igitur~~

~~$\varphi(1) \equiv 0$; $\varphi((\Delta 1)+(1)) \equiv 0$; $\varphi \Delta$~~ Erit itaque

$$A(1)^m + B(1)^{m-1} \ldots + N \equiv 0$$

$$A((\Delta 1)+(1))^m + B((\Delta 2)+(1))^{m-1} \ldots + N \equiv 0$$

$$\vdots \qquad \Delta 2 + (1) \ldots \qquad \vdots$$

Si potestates summarum $(\Delta 1)+(1)$ per seriem evoluantur, omniaque secundum potestates ipsius $\Delta 1$, $\Delta 2 \ldots$ ordinentur apparet proditurarum esse aliam expressionem huius formae

sive $a^{r\vartheta} \equiv 1$ (vbi $\vartheta < t$) sumatur k ita vt sit
~~a rk ≡ 1 (mod t)~~ $rk \equiv 1$ mod. t (quod fieri potest § 25)
~~Ob~~ $a^{r\vartheta} \equiv 1$ erit etiam $a^{rk\vartheta} \equiv 1$ (mod. p) et quia
$rk\vartheta \equiv \vartheta$ (mod t) erit (§ 42)
$a^{\vartheta} \equiv 1$ ~~contra suppositionem, qu~~
quod est absurdum quia a supponitur pertinere ad primam classem. Ex his colligitur theorema
dari totidem numeros qui ad potestatem t eleuari debent vt fiant $\equiv 1$, quot sunt numeri ~~primi~~ ad t primi, ipsum t non superantes.‡ Sic in exemplo nostro (§ 47) ~~ad pot~~ eleuandi sunt ad exponentes 1, 1; 2, 1; 3, 2; 6, 2; 9, 6; 18, 6. Conferantur quae §§. 35..38 explicauimus.

‡ siquidem datur vnicus

50.

Iam ope lemmatis (37 §) huius suppositionis veritatem facile corroborare poterimus. Sit modulus p; factoresque ipsius p−1 sint 1, e, f, g.........(p−1). Ex lemmate modo commemorati summa multitudinum numerorum ad 1, e, f &c. primorum ipsisque non maiorum erit = p−1. Si itaque reuera singulis factoribus 1, e, f..... totidem numeri adscribendi sunt quot docet theorema §. praec. omnes numeri ab 1 vsque ad p−1 erunt exhausti; at si suppositio nostra esset falsa, i.e. si vni alteriue factorum nullus conueniret, omnibus collectis ~~mult~~ pauciores

quam $p-1$ haberentur, i.e. unus aut alter numerorum ab 1 usque ad $p-1$ nulli factori esset adscriptus, quod cum § 47 consistere nequit. ~~Problema §~~ Theorema § praec. est itaque rigorose demonstratum: hinc etiam hoc:
Dantur tot numeri qui ad potestatem $p-1$ elevari debent quot ~~dantur nu~~ sunt numeri minores quam $p-1$ et ad $p-1$ primi.

51

haec ~~[illegible]~~ autem propositio maxime ~~[illegible]~~ est momenti

Quia demonstratio propositionis, quod semper dantur numeri quorum ~~omnes~~ potestates omnes inferiores quam $(p-1)$ ~~ta~~ non $\equiv 1$ est tam obvia quam primo aspectu videri posset, liceat etiam adicere a praec. aliquantum diversam, quandoquidem methodorum diversitas ad res obscuriores illustrandas plurimum valere solet. Semper discerpi potest. $p-1$ in factores huius formae a^α, b^β, c^γ, &c. ubi ~~a, b, c~~ a, b, c sunt numeri primi.. Iam dico I semper dari numer~~um~~os A, qui ad potestatem α^α evehi debet ut unitati fiat congruus, eodem modo alium B ~~(aut plures)~~ ad potestatem β^β elevandum &c &c.. II. ~~[illegible]~~ Productum $A.B....$ ex omnibus his numeris (aut eius res. minimum) ad potestatem $p-1$ evehi debere ut unitati fiat congruum. Has assertiones hoc modo demonstro:

I.1. Si nullus daretur numerus qui ad potestatem a^{α} evehi deberet omnes numeri ad potestatem $a^{\alpha-1}b^{\beta}c^{\gamma}\ldots$ sive $\frac{p-1}{\alpha}$ evecti unitati forent congrui.

Dem. Si quis assumto antecedente negaret consequens, ponamus ~~esse~~ non esse $z^{\frac{p-1}{\alpha}} \equiv 1$. Sit ~~exponens minimus infimae pot~~ potestas z^{t} infima, unitati congrua. t igitur ~~erit~~ metietur $p-1$ (§ 45), quotiens ~~ideoque~~ erit huius formae $a^{\alpha'}.b^{\beta'}.c^{\gamma'}\ldots$ ita ut α', β', γ' &c respective non sint maiores quam α, β, γ. &c. (demonstrationem perfacilem omittimus); at hunc $\frac{p-1}{\alpha}$ non metietur sive $a^{\alpha'-1}b^{\beta'}c^{\gamma'}\ldots$ erit fractio quod fieri nequit nisi sit ~~fiat~~ $\alpha'=0$. Quamobrem t factorem a^{α} involvere debet, eritque $a^{\alpha}M$. Facile hinc deducitur z^{M} ad potestatem a^{α} evehi debere ut ~~unitati fiat congruum~~ fiat $\equiv 1$, contra hypothesin.

I.2. At quoniam non omnes numeri ab 1 usque ad $p-1$ quorum multitudo est $p-1$ congruentiae $x^{(p-1):\alpha}$ satisfacere possunt, haec sequela locum habere nequit ~~non potest~~: hinc certum est dari numerum unicum saltem A, ~~qui~~ ad potestatem a^{α} ~~evehi debet~~ evehendus ut fiat $\equiv 1$. Ceterum ex uno dato facile ita ut §§ 48, 49 monstravimus ceteri derivantur omniumque multitudo sine negotio demonstratur esse $= (a-1)a^{\alpha-1}$ (§ 35). — Eodem modo demonstratur dari numeros B, C &c., ~~qui~~ quantaque ~~eorum~~ singulorum sit multitudo.

II. Ponamus productum $A.B.C....$ $(=M)$ ad potestatem t inferiorem quam $p-1$ evectum esse $\equiv 1$ sitque ~~$\frac{p-1}{t} = a^{\alpha'} b^{\beta'} c^{\gamma'} ....$~~

~~erit etiam M ad potestatem $t b^{\beta'} c^{\gamma'} d^{\delta'} ....$ evectum $\equiv 1$~~

~~At $\frac{p-1}{m} = a^{\alpha}$~~

erit t huius formae $a^{\alpha-\alpha'} b^{\beta-\beta'} c^{\gamma-\gamma'} ....$

Habebitur itaque etiam M ad potestatem $a^{\alpha-\alpha'} b^{\beta} c^{\gamma} ....$ evectum $\equiv 1$. At vero si numerus B ad hanc potestatem evectus (ob $\equiv$ propter ~~potestatem~~ $B^{b^\beta} \equiv 1$) erit $\equiv 1$; idem valet de C et factoribus sequentibus. Hinc colligitur

A ad potestatem $a^{\alpha-\alpha'} b^{\beta} c^{\gamma} ...$ elevatus $\equiv 1$ Ergo ~~hinc~~ $a^{\alpha-\alpha'} b^{\beta} c^{\gamma} ...$ per a^{α} dividitur, sive $b^{\beta} c^{\gamma} ....$ per $a^{\alpha'}$ quod est absurdum quia a est primus, qui nec b, nec c &c. metitur. —

Demonstratio posterior priori aliquantulum prolixior esse videtur. ~~At~~ contra prior ~~paullo~~ minus directa est. Posterior statim ~~simul patefacit~~ indicat quot numeri ad potestatem $p-1$ evehi debeant scilicet totidem, quot modis ~~diversis~~ productum $ABC...$ e diversis ipsorum A, B, C valoribus combinari potest, sive $(a-1)a^{\alpha-1}(b-1)b^{\beta-1}...$ Hoc eodem redit cum praeceptis (§§ 50 et 35)

55

Index quotientis $\frac{a}{b}$ ~~aequalis~~ (significatione generaliori §§) congruus est secundum $(t-1)$ differentiae indicum numeratoris et denominatoris.

Nam ~~Ind~~. quia ex defin. si $\frac{a}{b}$ ponatur $\equiv c$, $a \equiv bc$ erit $\text{Ind. } a \equiv \text{Ind. } b + \text{Ind. } c$ et $\text{Ind. } c \equiv \text{Ind. } a - \text{Ind. } b$

Hinc videtur ope tabularum indicum (quae tamen duplices esse deberent ut etiam ex indice numerus correspondens facile inveniri posset) omnes congruentias primi gradus facillime solvi, quia ~~ut capite~~ §§ demonstrabimus earum resolutio semper ad congruentias reduci potest in quibus modulus est numerus primus aut numeri primi potestas. ~~A~~ Sit ex. gr. $14x - 3 \equiv 0$ (mod 19) erit $x \equiv \frac{3}{14}$; $\text{Ind. } x \equiv \text{Ind. } 3 - \text{Ind. } 14 \equiv 6$. Hinc $x \equiv 7$

atque insuper ad modulos extendi deberent qui numerorum primorum sunt potestates de quibus ~~statim~~ mox loquemur

56

Ad analogiam designationis quotientium per $\sqrt[n]{a}$ (mod. p) ~~omnes~~ quemcunque valorem intelligemus qui congruentiae $a \equiv x^n$ (mod. p) satisfacit. ~~Nulla hinc ambigui~~ ut itaque haec expressio non modo radicem veram numeri a (si quam in integris habet) denotet, sed etiam radices numerorum ipsi a congruorum (eorum scilicet qui radicem rationalem revera admittunt.) Nulla hinc ambiguitas metuenda quia fractiones omnes, multo magis quantitates incommensurabiles hic penitus excluduntur: infra autem ubi ~~etiam aequation~~ de talibus quantitatibus sermo erit accurate cavebimus ne quis in signorum significatione haerere possit. — Si itaque $\sqrt[n]{a} \equiv x$ (mod p) erit $n\,\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,a$ (mod. $p-1$) debetque ad praecepta § tradita diiudicari, num haec congruentia resolutionem admittat, ~~quod~~ Scilicet si n habeat factorem communem cum $p-1$, f hic etiam Indicem. ipsius a metiri debet; quodsi hoc revera eveniat, f solutiones diversae erunt; hincque etiam $\sqrt[n]{a}$ aut f aut valores nullum ~~valorem~~ habebit.

Exempl. Quaeruntur valores expressionis $\sqrt[15]{11}$ (mod. 19) Soluenda igitur erit ~~n Ind. x~~ congruentia

$15\,\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,11 \equiv 12$ (mod 18)

~~Huius congru~~ inveniunturque valores $\mathrm{Ind.}\,x \equiv \left.\begin{matrix}2\\8\\14\end{matrix}\right\}$ (mod 18)

Hinc. valores ipsius x erunt: 4, 6, 9

57.

Quamvis haec methodus ad calculum sit expeditissima, obliuisci tamen non debemus eam esse indirectam. Attamen propter problematis eximiam utilitatem quaedam adhuc hic adiicere visum est quae ex principiis hactenus stabilitis deduci possunt. Infra capite 8 plura tradentur. Quia multitudo valorum expressionis $\sqrt[n]{a}$ si ulli dantur non ab a sed tantum a n pendet, considerabimus primo casum simplicissimum ubi $\sqrt[n]{1}$, quaeritur. Quia hoc casu debet esse $n\,\text{Ind.}\,x \equiv 0 \pmod{p-1}$ solutio semper erit possibilis. totque dabuntur valores ipsius x diversae quot unitates habebit maximus divisor communis ~~p~~ numerorum n et $p-1$. Quando itaque hi numeri inter se sunt primi unica solutio tantum dabitur scilicet $\text{Ind.}\,x \equiv 0$ et $x \equiv 1$. At si $n = \nu t$ et $p-1 = \pi t$ ita ut ν, π sint inter se primi, congruentia $\nu t\,\text{Ind.}\,x \equiv 0 \pmod{\pi t}$, t resolutiones admittet quae erunt $\text{Ind.}\,x \equiv 0, \pi, 2\pi \ldots (t-1)\pi$: erunt itaque valores ipsius x : 1, $(\text{rad. pr})^{\pi}$, $(\text{rad. pr})^{2\pi}$ &c. Hi valores igitur non pendent a ν sed tantum a t, valoresque expressionis $\sqrt[\nu t]{1}$ etiam erunt valores ex~~pressionis~~ huiusce: $\sqrt[t]{1}$ quandoquidem ν ad $\frac{p-1}{t}$ est primus.

Exempl. $\sqrt[15]{1}$ $(\text{mod } 19)$ tres valores habebit propter 3 maximam mensuram communem numerorum 15, 18, ~~hique inventi erunt~~ et adeos inveniendos investigandi erunt ~~qui simul erunt inventi erunt~~ valores huius expr. $\sqrt[3]{1} \pmod{19}$

Praeter 58

~~Casum~~ ubi $t=1$ qui per se est obvius hic etiam illum absolvere possumus ubi $t=2$. Quum enim $\sqrt[2]{}$ plures quam 2 valores diversos habere nequit, ~~huius expr.~~ hi erunt $+1$ et -1. Quare hi etiam ~~solutio congruentiae~~ erunt valores expr. $\sqrt[2\nu]{1}$ ~~[illegible]~~ ~~erit siquidem~~ quoties ν ad $\frac{p-1}{2}$ erit primus. Si itaque modulus eius sit indolis ut $\frac{p-1}{2}$ sit numerus primus, expressio $\sqrt[2m]{1}$ nullos alios valores admittit quam $+1$ et -1. ~~Tales moduli sunt 3, 5~~ Nisi forte $2m$ per $p-1$ sit divisibilis quo casu numeri quicunque ‡ valores expressionis esse possunt. Tales moduli sunt 3, 5, 7, 11, 23, 47, 59, 83 &c.

‡ per modulum non divisibiles

Quomodo ~~methodis~~ directis ~~de valoribus~~ expressiones superiores quales $\sqrt[3]{1}$; $\sqrt[4]{1}$ &c. tractari debeant infra docebitur.

59.

Sicuti hic ostendimus inventionem valorum huius expressionis $\sqrt[vt]{1}$ ad hanc reduci $\sqrt[t]{1}$, poterimus etiam in genere $\sqrt[vt]{a}$ ad hanc reducere $\sqrt[t]{a}$. Designemus valorem quemcunque ~~expressionis $\sqrt[vt]{a}$ per x atque~~ $p-1 = \pi t$, erit igitur

~~vt Ind $x \equiv$ Ind. a (mod πt)~~ $a \equiv x^{vt}$

Capiatur z ita ut sit $vz \equiv 1$ (mod. π) quod est possibile propter π ad v primum (hyp). ~~erit igitur~~

~~zvt Ind $x = z$ Ind $a = t$ Ind. x (mod πt)~~

~~Atqui si u est valor expr. $\sqrt[t]{a}$ erit t Ind u = ind a~~

Porro sit u unus valorum expressionis $\sqrt[t]{a}$ sive $u^t \equiv a$

Dico u^z fore valorem ipsius x, fit enim $u^{zvt} \equiv u^t \equiv a$.

(§

Sit Index ipsius $a \equiv t\alpha$ (namque si $\sqrt[t\nu]{a}$ valores reales habere supponitur haec indices debet esse forma); eruntque indices valorum expressionis $\sqrt[t]{a}$: $\alpha, \alpha+\pi, \alpha+2\pi, \ldots$ $\alpha+\pi(t-1)$. Sumatur z ita ut sit $\nu z \equiv 1 \pmod{\pi}$ quod fieri potest ob ν, π incommensurabiles; simul autem esse debet z et t incommensurabiles ‡ dico valores huius expressionis $(\sqrt[t]{a})^z$ ~~fore~~ exhibere omnes valores expressionis $\sqrt[t\nu]{a}$. Primo enim utrorumque multitudo est $= t$; ~~porro~~. Tum expressionis $(\sqrt[t]{a})^z$ valores, omnes erunt diversi. Binorum scilicet ~~quique~~ indices secundum πt erunt incongrui quia index $\alpha z + k\pi z$ non aliter huic $\alpha z + k'\pi z$ secundum πt congruus fieri potest quam si $k'-k$ per t dividatur sive $k' > t$ contra hypothesin. Denique quisue expressionis $(\sqrt[t]{a})^z$ valor exhibet valorem expressionis $\sqrt[t\nu]{a}$. nam $(\sqrt[t]{a})^{zt\nu} \equiv (\sqrt[t]{a})^t$ (§ 42) $\equiv a$. Q.E.D.

Exempl. Desideratur deducere valores $\sqrt[21]{2}$ (mod 31) e valoribus $\sqrt[3]{2}$. Est igitur $\nu = 7$, $\pi = 10$, $t = 3$, $\vartheta = 3$ faciendumque

$$7z \equiv 1 \pmod{10}, \quad z \equiv 1 \pmod{3}$$

Igitur $z = 13$, atque si uno alterove modo constant valores $\sqrt[3]{2}$ (qui sunt 4, 7; 20), habentur etiam valores

---

‡ quod facile ita obtinetur ut ponamus maximam ipsius t ~~inter π et t~~ mensuram ad π primam, $= \vartheta$ et faciendo $z \equiv 1 \pmod{\vartheta}$ $z \equiv$ numero cuique ad ϑ primo $\pmod{\vartheta}$ ex. gr. $z \equiv 1$

Haec methodo $\sqrt[n]{a}$ semper ~~directe~~ invenitur quando n et $p-1$ inter se sunt primi

$\sqrt[4]{2}$ qui scilicet essent $4^{13}, 7^{13}, 20^{13}$ i.e. ~~2, 9, 1~~ 2, 10, 19.

60.

Oportet nunc casum simpliciorem $\sqrt[t]{a}$ ubi t est divisor numeri $p-1$ accuratius evoluere. Vidimus hanc expressionem admittere t valores aut nullum; utrum autem eveniat, in genere hoc modo facile diiudicatur. Si ~~solutio~~ datur valor, debet esse $\text{Ind}.a = tm$; et si ut supra ponamus $p-1 = \pi t$ erit $\pi\,\text{Ind}.a = \text{Ind}\,a^\pi = \pi t m \equiv 0 \text{ mod}(\pi t)$ hinc $a^\pi \equiv 1 \,(\text{mod}.\,p)$. Si autem nulla solutio detur erit neq. Ind. a per t nec Ind a^π per πt divisibiles; et proinde a^π non erit $\equiv 1$. Sic in exemplo praec. §. invenitur valor

expr. esse $\sqrt[3]{2}$ possibilis propter $2^{10} \equiv 1 \,(\text{mod}.\,31)$; atque erit semper $\sqrt[2]{a}, \sqrt[3]{a}, \sqrt[4]{a} \ldots$ possibilis (i.e. dabuntur Quadrata, Cubi Biquadrata p ipsi a congrua) quando $a^{\frac{p-1}{2}}, a^{\frac{p-1}{3}}, a^{\frac{p-1}{4}} \ldots$ est $\equiv 1$ et inverse. Ita certo concludere possumus, $\sqrt[2]{(-1)}$ semper habere valores (binos) reales quando p est huius formae $4m+1$; contrarium autem evenire quando p est $4m+3$. nam $(-1)^{2m}$ semper $= 1$, $(-1)^{2m+1} = -1$.

Eximia haec veritas quae vulgo sic effertur: semper datur valor ipsius a ut $aa+1$ per p divisibilis fiat si $p = 4m+1$

et contra, hoc modo primum fuit demonstrata ab Ill. Eulero Nov. C. Petr. T. XVIII p. 1.. ad annum 1773.

Iam in tomo V Comm. Nov. qui a. 1760 publicatus est vir summus ~~professus est se~~ has res pertractavit; sed ipse fatetur demonstrationem se nondum absoluisse. — Eodem fere tempore etiam Ill. La Grange ~~idem~~ has res pertractavit, ~~ubi~~ exstatque demonstratio eius Nouv. Mem. de Berlin 1775. p.

Alia Demonstratio egregii huius theorematis, quae congruentiis exponentialibus non innititur infra ubi proprie de eo agendum erit ~~[illegible]~~ tradetur. (§)

61.

Postquam criterium dedimus ad quod facile cognosci possit utrum expressio $\sqrt[tt]{a}$ valores reales admittat necne, ~~enumeratimus quibus~~ docebimus quomodo hi valores revera directe investiganda sint. Primo ~~observam~~ videamus quo nexu hi valores diversi inter se cohaereant. ~~Ex principiis hactenus stabilitis sequitur~~ Indices horum valorum erunt radices congruentiae $tt\,z - \mathrm{Ind}.a \equiv 0 \pmod{p-1}$ unde concludimus (§29) si unus eorum sit ζ ceteros fore $\zeta + \frac{p-1}{tt}$; $\zeta + \frac{2(p-1)}{tt}$, $\zeta + \frac{3(p-1)}{tt}$ &c. Sunt autem ~~erunt eadem~~ $\frac{p-1}{tt}$, $\frac{2(p-1)}{tt}$ &c. indices valorum huius express. $\sqrt[tt]{1}$; si adeo hi valores per $\varrho, \varrho^2, \varrho^3$ designentur, omnes expressionis $\sqrt[tt]{a}$ valores erunt $\zeta, \zeta\varrho, \zeta\varrho^2$ &c.

Si ~~ex~~ ex. gr. $\sqrt[2]{a}$ habeat valorem ζ erit alter valor $-\zeta$. Omnes igitur valores talium expressionum inveniri nequeunt nisi simul constent valores expr. $\sqrt[t]{1}$.

62

Progredimur itaque nune ad evolutionem ~~casuum~~ subsidiorum, per quae quibus unus saltem valor expressionis $\sqrt[t]{a}$; ~~quem~~ quibus si ~~[illegible]~~ destituamur

directe inveniri possit

semper tamen ad huiusmodi expressionem ~~$\sqrt[t]{}$~~ $\sqrt[u]{1}$ reducere erit in potestate. ~~Ponamus~~ Illa vero ad haec redeunt. Ponamus unum valorem expr. $\sqrt[t]{a}$ ~~esse~~ exprimi posse per $\equiv a^{x}$, atque inquiramus in quibus casibus haec suppositio admittenda sit, et quomodo ~~t~~ x sit determinandum. Erit igitur ~~t~~ $u\,x$ Ind. a $\equiv$ Ind. a mod $(p-1)$. Ut haec congruentia ~~possibilis evadat debet esse maximus inter~~ divisor communis numerorum t Ind. a et $p-1$

#:

~~metiri debet hunc Ind. a. Ponatur $p-1 = \pi t$; Ind. a $= \alpha t$, atque maximus divisor communis numerorum $t\alpha$ et $\pi = \mu$ eritque maximus div. comm. numerorum $t\alpha$ et $t\pi$, $= \mu t$. Ergo hic igitur debet esse divisor numeri αt sive μ debet metiri ipsum α~~ Haec autem congruentia possibilis erit si t ~~ad~~ et exponens minimae potestatis ipsius a quae unitati est congrua ~~est~~ sint inter se ~~[illegible] numeros~~ primi; sin minus, impossibilis

---

In text. recep. Sit enim hic exponens $= e$ ~~et erit~~ sitque $p-1 = eu$ eritque Ind a $= ur$ ita ut rad e sit primus ($\S$) Hinc $txur \equiv ur$ (Mod eu). Habeant t et e divisorem communem maximum k et erit ~~divi~~ max. comm. moduli et coefficientis quantitatis ignotae ku quae ergo ur dividere debet. Hoc autem

57 ~~66~~

~~Ut conditiones ad huius congruentiae possibilitatem necessarias~~ ~~Ponamus~~ designemus ~~iam exponentem minimae potestatis numeri a quae unitati sit congrua per t, erit~~ ~~t~~ Ind. $a = m(p-1)$ ~~Ponamus iam p-1 = $A^\alpha B^\beta C^\gamma$~~.. ita ut t ad m sit primus.

Fit autem hinc $ux\, m(p-1) \equiv m(p-1)$ (mod $t(p-1)$) sive (§ infer.) $uxm \equiv m$ (mod. t) sive (§) $ux \equiv 1$ (mod. t) Haec igitur congruentia aequivalet priori, et quia ad eius possibilitatem requiritur ut t ad u sit primus, haec est conditio quaesita ~~ut quisque ipsius x valor~~ tunc autem a^x erit valor expressionis $\sqrt{a}$. Facile autem perspicietur ~~quemcunque~~ omnes ipsius x valores unicum tantum valorem dare posse.

63.

Quum autem ad hanc solutionem requiratur ut t sit notus videamus quomodo ~~huic rei~~ agere possimus hunc numerum ignorantes. ~~Iam facile patebit~~ Siquidem $\sqrt[u]{a}$ habeat valores possibiles ~~tum~~ $a^{\frac{p-1}{u}}$ ~~fore~~ ~~Quoniam~~ Sed quoniam $\equiv 1$ (mod. p), ~~unde sequitur~~ t ~~semper esse divisorem~~ metiri debet numerum $\frac{p-1}{u}$. ~~Iam si congruentia conditionalis~~ $ux \equiv 1$ (mod. t) supponatur esse possibilis t ~~ad~~ ~~productum~~ numerus primus erit ad productum e quotcunque factoribus ipsius u ~~erit~~ qualem per U designemus. At facile patet numerum $\frac{p-1}{u}$ nisi iam ad u sit primus, certo per repetitam divisionem per factores quos cum u communes habet illum reduci posse ut quotiens ad u sit primus. ~~Habe~~ Hinc ~~colligimus~~ nanciscimur numerum $\frac{p-1}{uU}$ ~~primum ad u~~ qui sit primus ad u simulque (ob U et t primos inter se) multiplum ipsius t. Sequitur vero e principiis capiti praecedente stabilitis, iis conditionibus hac ~~casu radices~~ congruentiam $ux \equiv t \pmod{\frac{p-1}{uU}}$ fore possibilem atque omnes eius radices una fore radices eiusdem congruentiae secundum modulum t, quarum unam cognovisse sufficit. Hinc colligitur quando ~~summus~~ aliquis valor expressionis $\sqrt[u]{a}$ per a^x exprimi possit, tum ~~x fore~~ pro x sumi ~~posse~~ licere radicem congruentiae

$$ux \equiv 1 \pmod{\frac{p-1}{uU}}$$

Exempl. Quaeritur $\sqrt[3]{6} \pmod{37}$. hic ergo ~~p-1 = 36~~ ~~u = 3~~ $\frac{p-1}{u} = 12$ et pro U sumi debet 3. hinc solvenda congruentia $3x \equiv 1 \pmod{4}$ cui satisfit ponendo $x \equiv 3$. Est vero $6^3 \equiv 31$ inveniturque revera $31^3 \equiv 6$ sive $31 = \sqrt[3]{6}$.

64. Probe autem meminisse oportet, has regulas nunquam applicare licere nisi conditio necessaria adsit; quodsi vero etiam hac deficiente uti iis ~~et~~ vellemus, semper in errorem delaberemur. Unico saltem casu de hac conditione semper securi esse possumus scilicet si $\frac{p-1}{u}$ iam ad u fuerit primus tum enim $U = 1$; t certo ~~erit divisor metietur numerum $\frac{p-1}{uU}$~~ utpote pars aliquota numeri $\frac{p-1}{u}$ ad u erit primus. Hoc igitur casu sine ~~alia~~ ulla incertitudine hanc methodum sequi possumus. At si $\frac{p-1}{u}$ ad u non sit primus, ~~tum potest~~ accidere potest ~~consequentiae~~ numeri quos regulas datas temere adhibendo elicimus veritati non sint consentanei, quod erit indicium conditionem illam

ut t ad u sit primus ~~non~~ habere locum.
~~Inquiramus~~ Quo igitur ~~qu~~ vinculo hi numeri cum veris cohaereant
~~ad saepe~~ videndum est: quae investigatio saepenumero emolumenta haud spernenda affert, Ponamus x ita esse determinatum ut supra: sed a^x non esse valorem expressionis $\sqrt[u]{a}$ i.e ~~seu~~ non esse a^{xu} ~~non esse~~ $\equiv a$. Quodsi unus tantum valor expressionis $\sqrt[u]{a^{xu-1}}$ inveniri potest quem vocemus, b erit $\frac{a^x}{b}$ (mod $p+1$) valor expressionis $\sqrt[u]{a}$. Namque posito hoc valore $\equiv c$ erit $a^x \equiv bc$; $a^{xu} \equiv b^u c^u$: at $b^u \equiv a^{xu-1}$ proin $a \equiv c^u$. ~~At vero simplicius esse expressionem $\sqrt[u]{b}$ quam $\sqrt[u]{a}$ ita apparebit~~. At vero quantum in genere simplicius sit invenire $\sqrt[u]{a^{(xu-1)}}$ ad quod hic quaestio est reducta, quam directe $\sqrt[u]{a}$ ita apparebit: Ostendimus his ambagibus numquam opus esse nisi t et U habeant factorem communem, qui consequenter erit minor quam t. Jam dico ~~hunc factorem communem~~ si a^{xu-1} ad potestatem evehatur cuius exponens est hic factor communis, prodire numerum unitati congruum; quum contra a ad potestatem maiorem, t, evehi oporteat. Illud autem sic demonstro. Sit $U = mv$, $t = ml$ et l et v inter se primi. Dico $(a^{xu-1})^m$ fore $\equiv 1$ sive quod idem est

t fore divisorem numeri $(ux-1)m$. Est enim $ux-1$ per $\frac{p-1}{uV}$ divisibilis (ex congruentia unde x deducitur seu $\frac{p-1}{uv}$) Superest igitur ut probemus t metiri ipsum $\frac{m(p-1)}{uV}$. Atqui t metitur ipsum $\frac{p-1}{u}$, v item, insuper autem est ad t primus hinc $\frac{p-1}{uvt}$ erit numerus integer Q.E.D.

Sed quid iuvat quod $a^{\frac{xu-1}{2}}$ ad minorem potestatem evehi debeat quam a ut unitati fiant congrui? Pauciores erunt numeri qui possunt esse a^{xu-1} quam ii qui possunt esse a, et quando secundum eundem modulum plures huiusmodi expressiones $\sqrt[u]{A}$ evolvere ~~convenit~~ occasio est id lucramur ut plurimas ex eodem fonte haurire possimus. Sic exempli gratia semper unicum saltem valorem expressionis $\sqrt[u]{A}$ (mod. 53) determinare possemus si modo sciamus valorem huius expressionis $\sqrt[2]{-1}$ qui est $\pm$ 23. Facile enim videtur ~~tales~~ tales expressiones semper directe inveniri posse excepto casu ubi $u=2$. Tum autem fit etiam $V=2$ et v non potest esse maior quam 2 unde quum omnes numeri qui ad potestatem 2 ~~evehi debeant~~ ut unitati fiant congrui sint $+1$ et -1, ad alias expressiones deferri nequimus nisi ad has $\sqrt[2]{\pm 1}$.

65

Ut omnia praecepta quae dedimus hic iterum ob oculos sistamus aliquot exempla adiecimus. Primum quaeratur valor ~~es~~ expressionis $\sqrt[9]{2}$ (mod 101). Fit ~~igitur~~ secundum §(59) $9z \equiv 1$ (mod 100) hinc $z \equiv 11$. et erit $2^{11} \equiv 28$ valor quaesitus. (§ 63)

Porro quaeratur $\sqrt[6]{6}$ (mod 101) faciendum est $3z \equiv 1$ (mod 50) Hinc $z \equiv 17$ et $6^{17} \equiv 65$ ~~et altera radix valor alter invenitur multiplicando hunc per~~ $\cancel{\sqrt[2]{1}}$ ~~i.e. per −1 eritque 36~~.

~~Quaeritur~~ $\cancel{\sqrt[8]{54}}$ ~~Fiat secundum~~ Reducitur itaque $\sqrt[6]{101}$ ad $\sqrt[2]{65}$ tentando tunc methodum praec. ponendum est $2x \equiv 1$ (mod 25) ~~mod~~ ideo $x = 12$; 65^{13} est $\equiv$ Sed hic numerus non est valor expressionis $\sqrt[2]{65}$. Est autem $\frac{\quad}{65} \equiv 100$, et $\sqrt[2]{100} \equiv \pm 10$; idcirco verus valor $\equiv 10$. $\equiv$

~~Ceter~~ Haec ~~sufficient de~~ sunt fere quae hic de determinatione talium expressionum hic tradi possunt. Non quidem est negandum methodos directas saepe esse satis prolixas: sed tale incommodum methodis directis plerumque incumbit; indirectae exercitato expeditiores. Sed quum de his loqui proprii non sit nostri instituti, quantum methodi directae in hoc genere polleant ostendere haud negligendum putavimus. Attamen de eo casu qui, nunc quidem, plurimum occurrere solet scilicet $\sqrt{A}$ iam agemus (Capite) et de his nihil amplius desideratum iri speremus.

66

Revertimur nunc ad radices primas quas diximus. Vidimus (§) radice prima tamquam pro basi assumta omnes numeros quorum indices ad $p-1$ sint primi item fore radices primas nullasque praeter has: unde simul earum multitudo sponte defluit. Nihil autem refert quamnam radicem primam pro basi assumamus. Sit numeri cuiusvis Q index $= q$ quando Basis est $= A$. Sit autem Index numeri A, si alia radix prima B pro basi assumatur, $\equiv a$ dico Indicem numeri Q in posteriori systemate fore aq. ~~...~~ Namque $B^{aq} \equiv (B^a)^q \equiv A^q \equiv Q$. Si autem A basis sit, erit a Ind. $B \equiv 1 \pmod{p-1}$ hinc Ind $B \equiv \frac{1}{a} \pmod{p-1}$ quae calculo exponentiali omnino sunt analoga. Si itaque tabula indicum pro basi A constructa, basi B adaptari debeat, determinandum est $\frac{1}{\text{Ind. } B}$ in Syst. pr. et per hunc numerum omnes Indices multiplicandi. — Si autem aliam basim ita determinari conveniat ut dato numero respondeat index datus, sit Index numeri in systemate priori e, Index autem in altero systemate $= \varepsilon$. Quaeratur valor $\frac{\varepsilon}{e} \pmod{p-1}$ qui nisi sint reales quaestio erit impossibilis. ~~Eligantur ii qui ad pr~~ Eligantur ii qui ad $p-1$ sunt primi; si etiam hi non adsint nulla datur radix prima quae pro basi assumi posset. Tum omnes numeri quibus in systemate dato hi valores sunt Indices pro basi assumi possunt.

~~In tabula ad~~ 67

Plerumque quidem prorsus arbitrarium est quamnam radicem pro Basi assumamus: at vero quibusdam casibus Basis ~~q~~ aliqua prae altera quaedam commoda praebere potest. In tabula huic capiti adiuncta basin ita determinavimus ut aut sit 10 si 10 est radix prima aut talis ut ~~[illegible]~~ Index numeri 10 (minimus) ~~indic~~ ~~qui~~ quam minimus i.e. sit submultiplum numeri $p-1$. ~~Hinc~~ Namque ~~app~~ si t sit exponens infimae potestatis ipsius 10 unitati congruae ~~fore Ind.~~ erit Ind. 10 valor expr. $\frac{p-1}{t}$ (mod. $p-1$) at minimus valor erit $\frac{p-1}{t}$ (abs.)

Quid hoc modo lucremur infra Cap. 7. explicabitur.

Ex. pro $p=53$ invenitur hoc modo $t=13$ hinc Ind. ~~[illegible]~~ 10 debet esse 4 i.e. ~~rad pr~~ Basis erit $\sqrt[4]{10}$, sed e valoribus huius expressionis 15, 27, 38, 26 primus et tertius ~~sunt~~ ~~[illegible]~~ Bases esse non possunt quia non sunt radices primae: at utrum ceterorum eligamus prorsus arbitrarium est: nos ut aliquid certi esset semper minimum valorem ~~eff~~ accepimus.

Methodi radices primas inveniendi maximam partem tentando innituntur. Si ea quae § 51 docuimus cum iis quae Capite 5 de congruentiarum $x^a \equiv 1$ solutione exponentur coniunget, ~~fere~~ omnes ~~id~~ quae methodorum directarum ~~vim fere~~ is inveniri possunt habebit. Neque videtur esse possibile in genere directe statim decidere utrum numerus propositus secundum modulum datum sit radix prima necne, ~~multo~~ ~~hoc minus quam~~ Euler. ~~Comm. Petrop.~~ Opusc. Analyt. T. I. p. 152 fatetur * Nihil itaque aliud agendum quam ut numerus quicunque tentetur et si forte non sit radix prima, alius numerus qui inter ~~eius~~ ~~priores~~ tentetur + residua priorum non occurrit: hi semper ita possunt combinari ut habeatur alius cuius periodus cycle sit maior quam periodi priorum: hocque modo progrediendum est donec ad numerum perveniatur cuius periodus sit quam maxima i.e. ad radicem primam. Plerumque compendia sese offerunt ad calculorum prolixitatem contrahendam: sed haec ~~non tam~~ difficilius ex praeceptis quam ex usu ediscuntur nec hic iis potest esse locus. Sufficiat unum exemplum adiicere ut aliquis alis inde conceptus formari possit.

*hos numeros assignare maxime difficile videtur eorumque indolem ad profundissima numerorum mysteria esse referendam

+ potestatum

69

Sit modulus propositus 61 quaeritur radix prima.
Tentetur primo numerus 3 nancisremur periodum

	1.	3	9.	27.	20.	60.	58.	52.	34.	[illegible] 51.	1.
Exp.	0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.

Quia itaque periodus numeri 3 est 10, 3 non est radix 65
prima Assumatur igitur alius ex. gr. 11 cuius periodus ita
procedit. 1. 11. 60. 3... Quia 60 occurrit inter periodum
numeri 3 statim congruentia formari potest. $11^2 \equiv 3^5$
Hinc si Index ~~d~~ numeri 3 assumatur $\equiv 6$ erit 2 Ind. 11 $\equiv$
30 et Ind. 11 aut $\equiv 15$ aut $\equiv 45$. Numerus 11 ergo non
est idoneus ad nonam positionem quia eius periodus est tantum
4. At ~~sumatur~~ producti 3.11 ~~hinc~~ Index erit aut
$\equiv 21$ aut $\equiv 51$, proin eius periodus $= 20$. Hinc habebimus

1.	33.	52.	17.	20.	50	3.	38.	34.	24.	60.	28	9.	44	41	11
0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
58	23	27	37	1											
16.	17.	18.	19.	20.											

Quia igitur 33 nondum est radix prima tentetur ~~ad~~ 4 qui
in periodo praec. non occurrit. Habebimus periodi initium

1 4 16 3 ... ~~Si igitur ponamus indicem numeri 33 =~~
0 1 2 3 ...

3 ~~erit~~. Hinc $4^3 \equiv 33^6$ et si Ind. numeri 33 ponatur $= 3$
erit 3 Ind. 4 $\equiv 18$ hinc Ind. 4 potest habere valorem
6, 26, 46 At 6 non potest esse Index numeri 4 quia iam
est Index numeri 33^2 sive 52. Ponamus igitur Ind. 4 esse
26. ~~Indices ... periodi praec. ... 30~~
4 itaque non ~~potest~~ est radix prima quia eius periodus habebit
30 terminos: at producti $4.33 \equiv 10$ Index erit $= 26 + 3 = 29$
qui cum ad 60 sit numerus primus 10 habebit periodum 60 terminorum

eritque adeo radix prima.

Ceterum in nostris calculis semper fere numerus 10 tentatus est quum eius periodus solvendo in fractionem decimalem $\frac{1}{p}$ perfacile obtineatur. Vid. Cap. 7.

70.

Antequam hoc argumentum deseramus propositiones quasdam adjungemus quae ope investigationum praecedentium perfacile absolvuntur.

~~Si 1, a, aa, a^3 ...... a^{t-1} sit ~~est~~ periodus potestatum numeri a secundum modulum p, productum~~

Productum ex omnibus periodi terminis secundum modulum quemcunque primum ~~...~~ erit $\equiv$ ~~...~~ $+1$, si terminorum multitudo est impar, et $\equiv -1$ si terminorum multitudo est impar.

Ex. 1, 2, 4 est periodus secundum 7, terminorum multitudo impar, et $1.2.4 = 8 \equiv +1 \pmod 7$

1.8.12.5. est periodus secundum 13, et productum $8.12.5 = 480 \equiv -1$ (mod. 13)

Demonstr. Periodi termini congrui sint potestatibus $1, a, aa \ldots$ ~~a~~ a^{t-1} ita ut a^t sit $\equiv 1$; erit productum $a^{1+2+3\ldots+t-1} = a^{\frac{t.t-1}{2}}$. Iam si t sit impar $t-1$ erit par et $\frac{t.t-1}{2}$ erit multiplum ipsius t. At si t fuerit par, erit $\frac{t.t-1}{2} \equiv \frac{1}{2}t$ (mod. t) ideoque $a^{\frac{t.t-1}{2}} \equiv a^{\frac{1}{2}t} \pmod p$ ~~ideoque~~ $\equiv -1$ (§ ins.)

71

Si hic pro a assumitur radix prima, periodus omnes numeros ab 1 usque ad p-1 comprehendet quorum igitur productum semper erit $\equiv -1$. (p−1 enim (et p primum) semper erit par, unico casu p=2 excepto: at hic residua +1 et −1 aequivalent). Hoc theorema satis elegans quod ita proferri solet: 1.2.3.....p−1 +1 semper per p dividitur quando p est numerus primus, a celeb. Waring primum est propositum ~~equiti aurato~~ armigero Wilson adscriptum. Medit. Algebr. p. Editio prima. p. 380 ed. 3. Waring adiicit: Demonstrationem huius propositionis eo magis difficilem esse quia nulla fingi possit notatio quae numerum primum exprimat*). At vero huiusmodi veritates non ex notationibus sed ex notionibus sunt hauriendae. — Post M. De la Grange non dedignatus est demonstrationem investigare quam Nouv. Mem. de l'Acad. de Berlin Annee 1771 derivit ex consideratione Coefficientium ex Evolutione producti $x+1.x+2.x+3\ldots\, x+p-1$. oriundarum. Scilicet si hoc productum sit $= X =$ $x^{n-1} + Ax^{n-2} + Bx^{n-3} \ldots + Mx + N$, Coefficientes A, B, ... M per p erunt divisibiles, N autem erit productum 1.2.3.....p−1. At pro x = 1, X per p erit divisibilis hinc etiam $x^{n-1}+N$ i.e. // Euler demi-rae mentionem facit

*) In praefatione ed. 3. demonstrationis La Grangianae mentio fit: sed in libro ipso locus hic non est deletus

$N+1$ per p erit divisibilis.

Postea ill. Euler in Opusculis analyticis T. I. p. 329 demonstrationem dedit quae cum ~~ro~~ nostra est eadem. ~~Post talium virorum~~
Quum tales viri hoc theorema suis meditationibus non indignum censuere, si aliam ~~eius~~ demonstrationem subjungo ~~non videbitur~~ nemini improbabitur.

Constat si p sit numerus primus tum congruentiam $ax \equiv 1 \pmod{p}$ semper unico tantum modo solui posse siquidem $a < p$, ~~tum~~ x autem semper posse capi $< p$. Hinc cuivis numero ipso p minori alius ~~dum~~ qui etiam ipso p est minor, adiunctus est, ut eorum productum unitati sit congruum, ill. Eulerus numeros socios appellavit. Si igitur ~~Ex his numeris: 1, 2, 3, 4 ... p−1 igitur bini~~ semper singuli ii numeri qui socios habent a se ipsis diversos cum suis sociis excerpantur ~~semper numeri excerpi poterunt quorum~~ a, A; b, B; c, C; ~~etc. ita ut $aA \equiv 1$; $bB \equiv 1$; $cC \equiv 1$~~ etc. Facile autem demonstrari potest nullos numeros sibi ipsis seu ipsorum socios fieri posse quam 1 et -1 sive quod hic idem est 1 et $p-1$ (Tales enim numeri congruentiae $xx \equiv 1 \bmod. p$ radices erunt; haec autem quum sit secundi gradus praeter $+1$ et -1 alias non admittit). Si igitur hi numeri ex his $1, 2, 3, 4 \ldots p-1$ excipiantur, ~~ii~~ qui eorum supererunt bini semper erunt associati. Hincque horum productum unitati erit congruum. At duorum reliquorum 1 et $p-1$ productum ~~est~~ est $\equiv -1$ Hinc $1.2.3 \ldots p-1$ erit $\equiv -1$. Q.E.D.

Ex. Sit $p = 13$: ~~Ex~~ Ex numeris $1, 2, 3 \ldots 12$, his 1 et 12 reiectis ceteri ita combinari possunt: $2,7$; $3,9$; $4,10$; $5,8$; $6,11$;

ita ut $2.7 \equiv 1$; $3.9 \equiv 1$ &c. Hinc . $2.7.3.9.4.10.5.8.6.11 \equiv 2.3.4.5.6.7.8.9.10.11 \equiv 1 \pmod{13}$ adeoque $1.2.3. \ldots 11.12 \equiv 12 \equiv -1 \pmod{13}$

72

Potest vero theorema in praec. § demonstratum generalius adhuc ita proponi. Productum ex omnibus numeris numero dato A minoribus ad eumque primis secundum hunc numerum A congruum est unitati vel ~~positive~~ negative vel ~~negative~~ positive sumtae. ~~Unitas~~ Unitas negative est sumenda si A est huius formae p^m aut huiusce $2.p^m$ ubi p est numerus primus a 2 diversus. Omnibus ceteris casibus unitas positive est sumenda. Facile videtur casum a Waringio prolatum sub priori contineri. — Demonstrationem huius theorematis quam quivis qui nostra principia bene tenuerit ~~[illegible]~~ sine difficultate eruet omittimus.

73

~~[illegible]~~ Revertimur ad enumerationem aliarum propositionum ad hoc argumentum pertinentium.

Summa terminorum periodi ~~omnium~~ completae est $\equiv 0$. ~~Quia~~ Sint enim periodi termini congrui terminis geometricae progressionis ~~$1, a, aa, \ldots a^t$~~ $1, a, aa, \ldots\ldots a^t$ ita ut $a^{t+1} \equiv 1$ erit summa progress. geom. $= \frac{a^{t+1}-1}{a-1}$ quae igitur erit $\equiv 0$ nisi forte $a-1 \equiv 0$ i.e. $a \equiv 1$ quem casum itaque excipere oportet quando unum ~~unum~~ adeo terminum periodum etiam vocare velimus

Productum ex omnibus ~~residuis~~ radicibus primis est $\equiv 1$ unico casu excepto ubi $p = 3$ (tum enim unica tantum datur radix prima $= 2$).

Dem. Si una radix prima pro Basi assumatur indices omnium radicum primarum erunt ii numeri qui ad $p-1$ sunt primi simulque hoc numero minores*. At facile videtur si K ad $p-1$ est primus tum etiam $p-1-K$ ad $p-1$ primum fore; ut ita bini constituant summam quae per $p-1$ est divisibilis. ~~Eodem~~ Unica casu datur exceptio scilicet si $K = p-1-K$ et ad $p-1$ numerus primus fieri potest, quod aliter evenire nequit nisi $K = \frac{1}{2}(p-1) = 1$ i.e. nisi $p = 3$.

* et proin indicis producti = summae ~~eo~~ numerorum ad $p-1$ primorum

74. Summa omnium radicum primarum erit $\equiv 0$, vel vel $\equiv -1$ vel $\equiv +1$ ~~eodem casu excepto ubi p~~

~~Dem. Sit $p-1 = a^\alpha b^\beta c^\gamma \ldots$ atque ita ut a, b, c etc. sint primi, sint porro $A, B, C, \ldots$ valores expressionum $\sqrt[a^\alpha]{1}$; $\sqrt[b^\beta]{1}$ &c. demonstravimus omnes radices primas sub hac forma contineri $A^m B^n C^p \ldots$ ita ut m, n, p respective sint $< \alpha, \beta, \gamma \ldots$ Hinc si $B^n C^p \ldots = V$ numerum quemcunque $B^n C^p \ldots$ denotet hae formae omnes radices primas comprehendent $AV, A^2V, A^3V \ldots A^{\alpha-1}V$; quorum igitur summa erit $A\Sigma V + A^2\Sigma V + A^3\Sigma V \ldots + A^{\alpha-1}\Sigma V = \frac{A^\alpha - A}{A-1}\Sigma V$. Eodem modo ΣV in productum solvi poterit~~

Expl. Demonstravimus supra si $p-1 = a^\alpha b^\beta c^\gamma \ldots$
~~tum~~ et A, B, C numeros tales qui ad potestatem $a^\alpha, b^\beta \ldots$
evehi debeant ut unitati fiant congrui tum quamvis radicem
primam ~~esse~~ residuum esse numeri hac forma contentis $A^a B^b C^c$ ~~si pro~~
ubi pro $a, b, c \ldots$ omnes numeri accipi debent
qui ad $a^\alpha, b^\beta \ldots$ respective sint primi hisque numeris minores.
Facile hinc deducitur aggregatum omnium numerorum sub hac
forma contentorum fore $\mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots$ si $\mathfrak{A}$ sit summa omnium
numerorum huius formae $A^a, B^b, C^c \ldots$ ~~Hinc demonstravimus~~
~~I°. Hoc productum adeoque summam omnium radicum primarum esse~~
~~$\equiv 0$ quando unus ex numeris $\mathfrak{A}, \mathfrak{B}, \mathfrak{C} \ldots$ fit $\equiv 0$. At $\mathfrak{A}$~~
Ostendimus $\mathfrak{A}$ esse $= \frac{A^{a^\alpha} - A}{A-1} - \frac{A^{a^\alpha} - A^a}{A^a - 1}$

At vero si $\alpha = 1$ erit $\mathfrak{A} = A + AA + \cdots + A^{a-1}$
$= (1 + A + AA \ldots + A^{a-1}) - 1$. Prima pars est periodus
completa: hinc $\mathfrak{A} \equiv -1$. At si $\alpha > 1$ erit $\mathfrak{A} =$
$(1 + A + AA \ldots + A^{a^\alpha - 1}) - (A^a + A^{2a} + A^{3a} \ldots + A^{a^\alpha - a})$
i.e. $=$ Differentiae duarum Periodorum adeoque $\equiv 0$. Hinc concludimus
Productum $\mathfrak{A}\mathfrak{B}\mathfrak{C} \ldots$ fore $\equiv 0$, ideoque etiam summam omnium
radicum primarum, si unus alterve ex numeris $\alpha, \beta, \gamma, \delta, \ldots$ fuerit > 1

i.e si $p-1$ per aliquod quadratum fuerit divisibilis, at $\equiv +1$ vel -1 si omnes numeri α, β, γ.. fuerint $=1$ i.e si $p-1$ per nullum quadratum dividitur et quidem $\equiv +1$ si numerus factorum primorum ipsius $p-1$ fuerit par, at $\equiv -1$, si ~~fue~~ impar. Hic tamen

ob exceptionem § 73 factor 2 non debet numerari

Exempl. Si $p = 5, 13, 17, 19, 29, 37, 41$ ex tabula annexa invenietur aggregatum radicum primarum $\equiv 0$

Si $p = 31, 43, 67, 71$ aggregatum $\equiv +1$

Si $p = 3, 7, 11, 23, 47$ aggregatum $\equiv -1$

Ceterum haec omnia clariora fient quum Cap. 8. de congruentiis agetur ~~[illegible]~~ quorum radices sunt haec radices primae

75

Quae hactenus exposuimus innituntur suppositioni ~~quod~~ modulum ~~sit~~ esse numerum primum. Superest ut eum quoque casum consideremus ubi numerus compositus pro modulo assumitur. Quia autem ~~hinc~~ hic plerumque nihil aliud opus ~~sit~~ est quam ut ~~[illegible]~~ ut principia nostra rite applicentur neque etiam proprietates tam elegantes, ~~[illegible]~~ quam ante, ~~[illegible]~~ hic locum habeant diu ijs immorari ~~necessarium~~ non erit necessum. Sufficiet ~~[illegible]~~ quae huic casui cum priori communia sint quaeque ~~[illegible]~~ illi propria exposuisse.

Theorema. $(h+\lambda p^{\mu})^{\vartheta p^{\nu}} - h^{\vartheta p^{\nu}} \equiv 0 \pmod{p^{\mu+\nu}}$ at ~~ver~~

$\equiv h^{\vartheta p^{\nu}-1}\vartheta\lambda p^{\mu+\nu} \pmod{p^{\mu+\nu+1}}$

~~praeter unicum casum p = 2 et μ = 1~~ Theorematis pars posterior locum non habet si $\mu = 1$ simulque $p = 2$. Ceterum μ hic semper > 0 assumitur.

Dem. Posset hoc theorema statim ex evolutione potestatis binomii deduci: ~~at quia~~ ostendendo omnes terminos post secundum per $p^{\mu+\nu+1}$ at ob ambages quas consideratio denominatorum in Coefficientibus requirunt, aliam methodum adhibemus.

Ponamus primo $\nu = 1$ eritque ob ~~(a+b)^μ ...~~

$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \&c.)$

$$(h+\lambda p^{\mu})^{\vartheta p} - h^{\vartheta p} = \lambda p^{\mu} \times \left((h+\lambda p^{\mu})^{\vartheta p-1} + (h+\lambda p^{\mu})^{\vartheta p-2}h + (h+\lambda p^{\mu})^{\vartheta p-3}hh \; \&c + +\right)$$

Quando igitur $\mu > 1$ ~~omnes termini~~ $(h+\lambda p^{\mu})$ erit $\equiv h \pmod{p^2}$. hinc secundum hunc modulum omnes termini parenthesi circumscripti erunt $\equiv h^{\vartheta p-1}$; quoniam vero eorum numerus sit $= \vartheta p$ omnes coniuncti erunt $\equiv \vartheta p h^{\vartheta p-1}$ i.e $= \vartheta p h^{\vartheta p-1} + C.pp$ hincque

$$(h+\lambda p^{\mu})^{\vartheta p} - h^{\vartheta p} = h^{\vartheta p-1}\vartheta\lambda p^{\mu+1} + C\lambda p^{\mu+2} \equiv h^{\vartheta p-1}\vartheta\lambda p^{\mu+1} \pmod{p^{\mu+2}}$$

Ut igitur theorema pro $\nu = 1$ constet. Iam si neges pro omnibus ipsius ν valoribus valere sit maximus pro quo verum sit $= \varphi$ ~~quorsum~~ ita ut pro $\nu = \varphi + 1$ fallat. Est igitur

$$(h+\lambda p^{\mu})^{\vartheta p^{\varphi}} - h^{\vartheta p^{\varphi}} \equiv h^{\vartheta p^{\varphi}-1}\vartheta\lambda p^{\mu+\varphi} \pmod{p^{\mu+\varphi+1}}$$

i.e. $(h+\lambda p^{\mu})^{p^\phi} = h^{p^\phi} + (\lambda + \mathfrak{C}p)p^{\mu+\phi}h^{p^\phi-1}$

Faciendo igitur $h^{p^\phi} = H$

$(h^{p^\phi-1})\lambda + \mathfrak{C}p = \Delta$ erit

$$(h+\lambda p^{\mu})^{\vartheta p^{\phi+1}} \equiv (H + \Lambda' p^{\mu+\phi})^{\vartheta p} \equiv H^{\vartheta p} + \Delta\vartheta p^{\mu+\phi+1}H^{\vartheta p-1} \pmod{p^{\mu+\phi+2}}$$

$$\equiv h^{\vartheta p^{\phi+1}} + h^{p^{\phi+1}-1}\vartheta\lambda p^{\mu+\phi+1} \pmod{p^{\mu+\phi+2}}$$

Ut igitur etiam pro $\nu = \phi+1$ valeat, nullusque provinde eius valor ~~maximus~~ pro quo sit verum detur. Unde theorema pro omnibus ipsius ν valoribus verum est. Q.E.D.

80.

Superest ut illum casum consideremus ubi $\mu = 1$. Potest vero eodem prorsus modo quo in § praec. sumus usi sine theor. binom. adiumento demonstrari

$$(h+\lambda p)^{\vartheta p-1} \equiv h^{\vartheta p-1} + h^{\vartheta p-2}(\vartheta p-1)\lambda p \pmod{p^2}$$

$$h(h+\lambda p)^{\vartheta p-2} \equiv h^{\vartheta p-1} + h^{\vartheta p-2}(\vartheta p-2)\lambda p \quad — \quad \&c.$$

unde omnium terminorum summa hocce casu erit

$$\equiv \vartheta p-1.\, h^{\vartheta p-1} + \frac{h^{\vartheta p-2}\lambda\,\vartheta p-1.\,\vartheta pp}{2}$$ quod semper

est $\equiv \vartheta p-1.\, h^{\vartheta p-1}$ (mod p^2) unico excepto casu $p=2$ quem postseorsim considerabimus. Quae sequuntur hocce casu ut in ceteris procedunt. Unde casu $p=2$ praetermisso habemus generaliter

$$\cancel{(h+\lambda p^{n-k})^{\vartheta p^k} \equiv h^{\vartheta p^k} \pmod{p^{n+k}}}$$

$$\cancel{(h+\lambda p^{n-k-1})^{\vartheta p^k} \text{ non } \equiv h^{\vartheta p^k}}$$

$$(h+\lambda p^{\mu})^{\vartheta p^{\nu}} \equiv h^{\vartheta p^{\nu}} \pmod{p^{\mu+\nu}}$$

$(h+\lambda p^{\mu})^{\vartheta p^{\nu}}$ non $\equiv h^{\vartheta p^{\nu}}$ (mod. qui est altior ipsius p potestas quam haecce $p^{\mu+\nu}$) quando λ, ϑ et h ad p sunt primi

Hinc statim fluunt propp. 1. et 2 quae in § 78 demonstrandae nobis supererant. Nam

I. Si $h^{\theta e p^k} \equiv 1$ erit etiam $(h+\lambda p^{n-k})^{\theta e p^k} \equiv 1 \pmod{p^n}$

II. $H^{\theta e p^k}$ non fore $\equiv 1$ si $H \equiv h$ mod. p non autem $H \equiv h$ mod. p^{n-k}

Sit enim $H = h + \lambda p^{n-k-z}$ ita ut λ ad p sit primus et $z > 0$ eritque

$H^{\theta e p^k}$ non $\equiv 1$ pro modulo qui est ~~maior~~ altior ipsius p potestas quam p^{n-z} sive pro modulo p^n. Q.E.D.

81.

~~Haec iam ad nostrum propositum sufficere possent~~

Quum nunc, per praec. demonstratum sit congruentiae $x^t - 1 \equiv 0$ numerum radicum mod p^n maximum ~~[illegible]~~ ipsorum p^n et t divisorem communem superare non posse multo minus ipsum t, (excepto casu $p=2$), omnia quae §§ 48–51 ~~de~~ pro modulis

primis nostro etiam casu valent egregiaque inde veritas
fluit ~~radices~~ primos dari non solum pro ~~radicibus~~ modulis primis
sed etiam pro modulis qui numerorum primorum sint potestates.

Hic vero radices primitivi sint qui ad potestatem $p^n p-1$ debent elevari ut unitati fiant congrue sive in quarum periodo omnes numeri occurrunt ad p^n primi.

Omnia autem quae postea de indicibus eorumque ~~usu~~
tradidimus, porro de congruentiarum $x^t - 1 \equiv a$ solutione
&c ad hunc casum etiam applicari possunt, paucula immutatione
facta ~~quae ideo requirit~~ quod ~~pro~~ loco $p-1$ hic semper $p^n.p-1$
considerari debeat. Quum itaque haec nullam ~~insignem~~ difficultatem
habeant ~~neque in sequentibus magnus eorum usus fiet haec~~ iis
quos libet ~~evolvenda~~ linquimus. ~~Unum autem adhuc adiicere~~
~~debemus scilicet methodum directam solutionem~~ radices
~~congruentiae $x^t \equiv 1 \pmod{p^n}$ ex eiusdem congruentiae radici-~~
~~bus secundum modulum p deducendi~~ omnia ex integro

~~82~~.

~~Ne infra opus habeamus~~
Repetere plane superfluum foret. Id tantum observamus
~~plerumque omnes~~ radices congruentiae $x^t \equiv a$ ~~##~~ secundum modulum
p^n ex radicibus eiusdem congruentiae secundum modulum
p facile deduci posse: quum autem reductio huiusce ~~haec~~ congruentiae parum sibi proprii
habeat, de ea loquemur quum de reductione congruentiarum quarum-
cunque agemus Cap VIII. Superest igitur tantum ut
~~[illegible]~~ ~~[illegible]~~ de modulo 2^n adhuc quaedam adiiciamus.

~~Veritates ...~~ Propositiones quae pro hoc casu nullam exceptionem patiuntur sunt:

$$x^{2^{p-1}} \equiv 1 \pmod{2^p}$$

$$(h+2^\mu\lambda)^{\theta 2^\nu} \equiv h^{\theta 2^\nu} + h^{\theta 2^\nu - 1}\lambda\,\theta\, 2^{\mu+\nu} \pmod{2^{\mu+\nu+1}}$$ quando

$\mu > 1$ sive $(h+2^\mu\lambda)^{\theta 2^\nu} - h^{\theta 2^\nu}$ in hoc casu per $2^{\mu+\nu+1}$ non dividitur (§ 79). si λ et h et θ sint impares.

Hoc autem pro $\mu = 1$ ~~hoc~~ subsistere non posse vel inde clarum quod tunc $(h+2\lambda)^{\theta 2^\nu} - h^{\theta 2^\nu} = \pm\left(-h + 4\frac{h-\lambda}{2}\right)^{\theta 2^\nu} - (-h)^{\theta 2^\nu}$ quod si modo $\nu > 0$ ob h et l impares, proinque $\frac{h-\lambda}{2}$ = numero integro sub formula superiori ubi $\mu = 2$ continetur unde $(h+2\lambda)^{\theta 2^\nu} - h^{\theta 2^\nu}$ per $2^{\nu+2}$ dividitur quin etiam ~~non vero per~~ si $\frac{h-\lambda}{2}$ non fuerit impar altiori. Hinc statim sequitur $(1+2\lambda)^{2^{n-2}}$ ~~per 2^n~~ esse $\equiv 1$ quidquid sit $\lambda \pmod{2^n}$ $n > 2$ nullusque datur numerus qui ad potestatem 2^{n-1} evehi debeat ut unitati fiat congruus seu cuius periodus omnes numeros impares amplectatur. Perinde facile perspicitur $\mp 1 + 4\lambda$ si ~~...~~ fuerit impar ad potestatem p^{n-2} evehi debere ut unitati fiat congruus (mod. p^n) ; i.e. eius periodus dimidium omnium numerorum imparium ipso p^n minorum amplectitur. ~~Omnes hi numeri in duas~~

Jam clarum est numerum huius formae $8n+3$
1 quadratum habere huius formae $8n+1$; cubum iterum formae
$8n+3$ &c Unde eius periodus omnes numeros harum formarum
$8n+1, 8n+3$ complecti debet. Simili modo periodus numeri

formae	complectetur omnes numeros formae
$8n+5$	$8n+1, 8n+5$
$8n+7$	$8n+1, 8n+7$

— ~~Inque~~ Generaliter potestas ~~dati~~ numeri propositi quae unitati sit congrua facile ita determinatur:
Ponatur sub hanc formam $\pm 1 + 2^{\mu}\lambda$ ita ut λ sit impar et $\mu > 1$. Jam si modulus sit 2^n numerus evehi debet ad potestatem

$2^{n-\mu}$ si $n > \mu$

$\left.\begin{matrix}1\\2\end{matrix}\right\}$ si $n =$ sive $< \mu$ $\begin{matrix}\text{pro signo superiori}\\ \text{pro signo inferiori}\end{matrix}$

84.

~~De modulis qui sunt numeri e diversis primis compositi pauca sunt~~ ~~non est quod multa~~ quae moneamus
~~De congruentiis x^t ... $\equiv$~~ De residuis functionum exponentialium secundum modulum e pluribus primis compositum pauca sunt quae non de congruentiis in universum valeant: ~~quare iis hic immor~~ quod quum infra fusius docebitur non est quod iis immoremur. Observamus tantum bellissimam proprietatem ~~congr~~ quae modulis supra consideratis convenit, scilicet existentiam radicum primarum hic locum non habere nisi unico casu ubi modulus

est duplum numeri primi; ~~Quando~~ Si enim modulus sub hanc formam ponatur $m = a^\alpha b^\beta c^\gamma \ldots$ ita ut $a, b, c \ldots$ sint numeri primi ~~erit per quemcunque~~ z autem ad m sit primus, ~~erit atque~~ denique $a^{\alpha-1}(a-1)$ designetur per A, $b^{\beta-1}(b-1)$ per B &c. erit

$z^A \equiv 1 \pmod{a^\alpha}$

$z^B \equiv 1 \pmod{b^\beta}$

&c

Si igitur M sit minimus numerus qui per $A, B, C \ldots$ sit divisibilis erit etiam

$z^M \equiv 1 \pmod{a^\alpha}$

$z^M \equiv 1 \pmod{b^\beta}$ &c

adeoque $z^M \equiv 1 \; (\cancel{\text{mod}}\; a^\alpha b^\beta \ldots = m)$ et z^M erit minima potestas ~~ad quam z per~~ ipsius z unitati congrua. At nisi $m = 2p$ M semper erit minor quam $\cancel{\,}$ $ABC\ldots$ (quia semper A, B, C erunt commensurabiles) nullusque igitur (praeter casum memoratum) datur numerus qui ad potestatem $ABC\ldots$ evehi deberet ut unitati fieret congruus, seu cuius periodus omnes numeros ad m primos (quorum multitudo est $ABC\ldots$) complecteretur. — Sic exempli gr. pro modulo $1001 = 13.11.7$ omnes numeri ad potestatem cuius exponens est 60 evecti erunt $\equiv 1$ quia 60 est minimus dividendus numerorum 12, 10, 6. Utemur hac proprietate infra. — Casus autem $m = 2p$ prorsus ~~...~~ similis est ei ubi modulus est numerus primus.

85.

Literatura

Tabula exhibens Indices numerorum primorum pro modulis qui sunt numeri primi aut primorum potestates.

	3	5	7	9	11	13	17	19
Bas.	2	2	3	2	2	2		
2	1	1	2	1	1			
3		3	1	–	8			
5			5	5	4			
7				4	7			
10					5			
11								
13								
17								
19								
23								
29								
31								
37								
41								
43								
47								
53								
59								
61								
67								
71								
73								
79								
83								
89								
97								

Caput quartum

De residuis functionum secundi gradus

86

Theor. Si omnia quadrata successiva ~~numerorum naturalium quadrata~~ secundum modulum quemcunque m ad residua sua minima reducantur plura quam $\frac{1}{2}n+1$ sive $\frac{1}{2}(n+1)$ adesse non possunt.

Dem. Fiant quadrata numerorum a cifra ~~ab unitate~~ incipientium

$$0, 1, 2^2, 3^2 \ldots\ldots (m-3)^2, (m-2)^2, (m-1)^2, mm, (m+1)^2, (m+2)^2 \text{ \&c}$$

Jam facile elucet

$$(m-1)^2 = (1-m)^2 \equiv 1$$
$$(m-2)^2 = (2-m)^2 \equiv 2^2$$
$$(m-3)^2 = (3-m)^2 \equiv 3^2$$
$$\&c$$

Sive omnes numeri quorum summa $= m$, habent quadrata congrua. ~~Quando igitur m est impar~~ Ergo, residua quadratorum ~~quadrata~~ post $(\frac{1}{2}m)^2$ ordine inverso revertentur scilicet si m est par $(\frac{1}{2}m+1)^2 \equiv (\frac{1}{2}m-1)^2$; $(\frac{1}{2}m+2)^2 \equiv (\frac{1}{2}m-2)^2$ &c, si vero m impar erit $(\frac{1}{2}m+\frac{1}{2})^2 \equiv (\frac{1}{2}m-\frac{1}{2})^2$; $(\frac{1}{2}m+1\frac{1}{2})^2 \equiv (\frac{1}{2}m-1\frac{1}{2})^2$ &c

Si itaque omnia residua quadratorum a 0 usque ad $(\frac{1}{2}m)^2$ sive $(\frac{1}{2}m-\frac{1}{2})^2$ colligantur (quorum numerus est $\frac{1}{2}n+1$ vel $\frac{1}{2}(n+1)$) omnia quae sunt possibilia iam habebuntur; namque post mm

residua eodem ordine redeunt ut ab initio (§14)

87.

Ex. Secundum modulum 11 haec habebuntur residuorum periodus: 0, 1, 4, 9, 5, 3; 3, 5, 9, 4, 1, 0; 1, 4, 9 &c
Sunt igitur secundum hunc modulum ~~et~~ omnes numeri qui alicui horum sex non sunt congrui: 0, 1, 3, 4, 5, 9 nulli quadrato congrui fieri possint.

sive ~~et~~ qui congrui sunt uni ex his 2, 6, 7, 8, 10

Secundum modulum 15 haec residua provenient:
0, 1, 4, 9, 1, 10, 6, 4; 4, 6, 10, 1, 9, 4, 1, 0; 1, 4, 9 &c Nulli igitur numeri ~~et~~ secundum modulum 15 quadrato possunt fieri congrui qui alicui ex his sunt congrui:
2, 3, 5, 7, 8, 11, 12, 13, 14.

Hinc colligitur ~~omnes numeros~~ pro quovis modulo dato omnes numeros in duas classes distingui quarum altera contineat eos qui quadratis congrui fieri possunt, altera eos qui nullo modo possunt. Illos appellabimus *Residua quadratica moduli dati*, hos autem *Non-Residua quadratica*; Brevitatis gratia vero quando ~~quia hoc~~ ~~capite~~ nulla ambiguitas inde potest oriri illos simpliciter moduli Residua, hos Non residua ~~a~~ dicemus

Ceterum etiam hoc capite initium a modulis primis faciemus ideoque hoc in sequentibus semper intelligendum usque ad

88 exnumeris

~~Si~~ Si modulus sit numerus primus p, ~~totidem~~ ~~totidem~~ ab 1 usque ad $p-1$, ~~dimidium~~ totidem erunt residua quot nonresidua i.e. $\frac{p-1}{2}$.

Facile scilicet probatur omnia quadrata ab 1 usque ad $\left(\frac{p-1}{2}\right)^2$ esse incongrua proinque ~~resi~~ omnia residua ~~ex~~ illis diversa. Si enim fieri posset ut ~~r et~~ ρ $r^2 \equiv \rho^2$ ac tam quam ~~et~~ $r < \frac{p-1}{2}$, illaque $> \rho$, foret $(r-\rho)(r+\rho) \equiv 0$. Hoc autem fieri nequit quia tam $r-\rho$ quam $r+\rho$ sunt $< p$ (§.17). — Hinc multitudo residuorum erit $\frac{p-1}{2}$, adeoque multitudo non residuorum $= p-1-\frac{p-1}{2} = \frac{p-1}{2}$.

Monere hic convenit ~~et~~ cifram ab investigationibus praesentibus excludi; ~~cum~~ ~~quae~~ sideoque omnia quadrata quorum radix per p est divisibilis, quum hic casus ~~semper~~ taediosas per se sit clarus, ~~cumque~~ nosque tantum ~~taediosas~~ cogeret exceptiones afferre. Eadem de causa modulus $= 2$ hic plane non consideratur.

89.

Quia ea quae in Cap. praec. pertractavimus magnam ~~semper~~ lucem etiam in his affundere possunt semper nexum ostendere perutile erit. Patet vero ~~autem~~ facile omnes numeros quadratos sive quadratis congruos indices habere pares eos contra qui quadratis nullo modo fieri possunt congrui indices impares habere debere

Hinc quia ob $p-1$ parem tot semper dantur indices pares quot impares ~~etiam~~ theorematis praecedentis veritas statim illucet.

Ex. Pro modulis	Erunt Residua	Non Residua
3	1	2
5	1.4	2.3
7.	1.2.4.	3.5.7
11	1.3.4.5.9	2.6.7.8.10
13.	1.3.4.9.10.12	2.5.6.7.8.11
	&c.	

90

Productum e duobus residuum erit; sed productum e residuo in nonresiduum erit non residuum: denique productum e duobus non residuis erit ~~non~~ residuum.

Demonstratio I. sint A, B residua e quadratis aa, bb oriunda; sive $A \equiv aa$, $B \equiv bb$ hinc $AB \equiv aabb \equiv (ab)^2$; i.e. Residuum.

II. Sit $A \overset{\text{residuum}}{\equiv} aa$: B autem Non residuum. Iam si AB foret residuum: ponamus $AB \equiv hh$. Quaeratur $z \equiv \frac{h}{a}$ (mod. p); ~~eritque~~ itaque $aazz \equiv hh$ ~~Quoniam~~ vero $aaB \equiv hh$ erit $B \equiv zz$ seu B foret Residuum contra hypothesin.

~~III. Sint A, B Non residua, eritque AB residuum~~

~~Hinc iam deducitur statim si omnia $\frac{p-1}{2}$ residua per aliquod~~ Si itaque

quodcunque Non residuum multiplicentur haec $\frac{p-1}{2}$ producta erunt Non residua, omniaque inter se incongrua

Haec sunt quae etiam sine profundiorum investigationum adiumento e primis principiis erui possunt. Antequam autem ulterius ~~progredi~~amur de ~~veris~~ modulis compositis agere necesse est.

§ Theorema § 86 quidem universaliter est demonstratum. ~~Moduli hinc~~ Abhinc vero convenit modulos qui numerorum primorum sunt potestates ab iis separare qui e numeris primis diversis sunt compositi. Sit igitur modulus p^n et a huius moduli residuum per p non divisibile sit $a \equiv \alpha^2$. Tum praeter α et $p^n - \alpha$ nulli numeri infra p^n quadrata habent ipsi a congrua. Namque si $f < p^n$ $f^2 \equiv$ ~~α^2 mod~~ $a \equiv \alpha^2$ (mod p^n) erit $(f-\alpha)(f+\alpha) \equiv 0 \pmod{p^n}$. ~~Tum si fiat $f = a$ per~~ f Hoc autem fieri nequit nisi sit

I. aut $f-\alpha$ per p^n divisibile: tum numerus f non potest esse diversus ab α.

II aut $f+\alpha$ per p^n divisibile tum vero f non potest esse diversus a $p^n-\alpha$

III aut $f-a$ divisibilis per p^μ et $f+a$ divisibilis per p^ν ita ut $\mu+\nu = n$ et tam μ quam $\nu > 0$.

At si esset $f+\alpha$ per p^μ itaque etiam per p, insuperque $f-\alpha$ per p divisibilis; foret etiam $(f+a)-(f-a) = 2a$ per p divisibilis adeoque etiam a contra hypothesin [nam cum ~~…~~ $p=2$

huc non considerari iam monuimus.) Unde constat propositio.

94.

~~Hinc~~ ~~Quum igitur~~ ex omnibus numeris ipso p^m minoribus per p non divisibilibus, quorum $p^{n-1}\overline{p-1}$ bini semper idem suppeditent residuum, ~~tot~~ $\frac{1}{2}p^{n-1}\overline{p-1}$ residua orientur quae omnia per p non erunt divisibilia. Altera autem semissis talium numerorum erunt Non Residua quum pateat m ~~eos~~ ex quadratis numerorum per p divisibilium numeros tales ~~fieri~~ produci non posse; i.e. inter hos numeros totidem erunt Non Residua quot residua. Quod ~~proprietas~~ theorema etiam ex proprietatibus indicum perinde ut § dedici potuisset. Ita pro modulo 27 hi numeri erunt residua 1, 4, 7, 10, 13, 16, 19, 22, ~~25~~, 25; hi vero non residua 2, 5, 8, 11, 14, 17, 20, 23, 26. utrorumque multitudo $= \frac{1}{2}\cdot 3^2\cdot 2 = 9$.

At facile patet non residuum moduli p etiam fore non residuum moduli p^n (qui enim numerus secundum p^n quadrato est congruus, eidem quadrato etiam secundum p erit congruus). ~~Quia autem~~

~~in quovis intervallo inter 0 et p, ~~fiunt secund~~ p et $2p$, $2p$ et $3p$ ... p^n ~~$(p-1)p^{n-1}$~~, $p^n - p$ et p^n, sint. $\frac{p-1}{2}$ ipsius p non residua ~~inter~~ (per p non divisibilia), inter 0 et p^n erunt $\frac{1}{2}(p-1)p$~~

Aeque facile quisquis videbit ~~inter~~ ~~infra p^n fore $\frac{1}{2}p$ vel~~ numerorum infra p^n ~~per~~ per p non divisibilium, semissem fore moduli non residua

quae igitur eadem erunt cum non residuis ipsius p^n
Quia ergo p^n alia non residua habere nequit nisi quae simul sint non residua ipsius p sequitur.
<u>omnia ipsius p^π residua, simul ipsius p^n i.e cuiuscunque ipsius p potestatis ~~alia~~ residua esse</u> (semper exclusis iis quae p metitur).

95.

Quod autem attinet ad numeros per p divisibiles patet eorum quadrata ~~etiam~~ per p^2 fore divisibilia adeoque ~~nul~~ omnes numeros per p quidem divisibilia non vero per p^2 ipsius p^n (ubi $n > 1$) fore non residua. Generaliter autem si proponatur $p^k A$ ubi p ipsum A non metitur hi casus erunt distinguendi

1. Si k sit $=$ sive $> n$ erit $p^k A \equiv 0 \pmod{p^n}$ ideoque residuum,
2. Si k sit $< n$ et impar. ~~Tunc patet $p^{2\lambda+1}$~~ Tunc erit $p^k A$ non residuum. Si enim esset $p^k A = p^{2\lambda+1} A \equiv ss$ i.e $p^{2\lambda+1} A - ss$ per p^n ideoque (ob $n > 2\lambda+1$) etiam per $p^{2\lambda+1}$ divisibile s necessario per ~~$p^{\lambda+1}$ deberet esse divisibilis~~ esse huius formae $p^{\lambda+1}\sigma$. Tunc vero $p^{2\lambda+1}A - ss$ fit $p^{2\lambda+1}(A - \sigma\sigma p)$. Quia igitur (hyp.) A (per p non dividitur adeoque etiam) $A - ssp$, $\times$ $p^{2\lambda+1}$ deberet per p^n dividi, minor per maiorem Q.E.A.
3. Si k sit $< n$ et par. Tum erit Ap^k residuum ipsius p^n vel non-residuum prout A fuerit ipsius p residuum vel non residuum.

Namque $Ap^{2\lambda}$ aliter quadrato ss congruum esse nequit (mod p^n) nisi
posito $s = p^\lambda \sigma$. Ut vero sit $Ap^{2\lambda} \equiv p^{2\lambda}\sigma\sigma$ debet esse
$A \equiv \sigma\sigma$ (mod. $p^{n-2\lambda}$) ~~quod est possibile vel~~ i.e. A residuum
ipsius $p^{n-2\lambda}$ sive ob A per p indivisibilem residuum ipsius
p (§ praec). Unde ~~statim fluit~~ constat assertum.

96.

Judicium de residuis et nonresiduis moduli primi potestas qui est numeri
reducitur itaque omnino ad casum ubi modulus est nume-
rus primus. Superest casus ubi modulus ubi modulus
e numeris primis diversis est compositus. Sit itaque modulus $m =$
$a^\alpha b^\beta c^\gamma \ldots$ ~~A~~ Quivis ut N sit residuum ...
$N \equiv xx$ secundum hunc
secundum singulos factores tam sing.
ad N debet esse residuum ~~ipsius~~
quod ~~secundum~~ praecepta §§ praec. diiudicatur.
Quarum conditionum si una
residuum ipsius m. Facile
esse sufficientes. Si enim sit

$$N \equiv A^2 \text{ mod. } a^\alpha$$
$$\equiv B^2 \text{ mod. } b^\beta$$
$$\equiv C^2 \text{ mod. } c^\gamma \text{ \&c}$$

capi
x ...
$x \equiv$
$\equiv$
$\equiv$

~~hic ipsius x~~
x omnibus congruentiis satisfaciet
$N \equiv xx$ (modd. $a^\alpha, b^\beta, c^\gamma \ldots$)
$N \equiv xx$ (mod m).

Ceterum cuivis hanc deductionem attente ponderanti statim patebit: Cum numeri A, B, C &c. tam positive quam negative accipi possint sive quod idem est ~~etiam~~ tam hi numeri ipsi quam eorum complementa ad $a^\alpha, b^\beta, c^\gamma$ &c respective, 2^μ diversas combinationes ~~ad~~ adeoque 2^μ diversos ipsius x valores inde oriri si μ sit multitudo factorum $a^\alpha, b^\beta, c^\gamma \ldots$ ~~Fusius de~~ Fusius et generalius de hoc argumento in Cap. VIII agetur.

Namque $Ap^{2\lambda}$ aliter quadrato ss congruum esse (mod p^n) nequit nisi posito $s = p^\lambda \sigma$. Ut vero sit $Ap^{2\lambda} \equiv p^{2\lambda}\sigma\sigma$ debet esse $A \equiv \sigma\sigma$ (mod. $p^{n-2\lambda}$) ~~quod est possibile vel~~ i.e. A residuum ipsius $p^{n-2\lambda}$ sive ob A per p indivisibilem residuum ipsius p (§ praec). Unde ~~statim fluit~~ constat assertum.

96.

Judicium de residuis et non-residuis moduli primi potestas qui est numeri reducitur itaque omnino ad casum ubi modulus est numerus primus. Superest casus ubi modulus ubi modulus e numeris primis diversis est compositus. Sit itaque modulus $m = a^\alpha b^\beta c^\gamma \ldots$ ~~A~~ Quaus ut ~~A~~ sit residuum sive ut sit ~~A~~ $N \equiv xx$ secundum hunc modulum, haec congruentia etiam secundum singulos factores locum habere debet i.e. N debet esse residuum ~~ipsius~~ tum singulorum modulorum a^α, ~~quam ipsius~~ b^β, c^γ &c

quod ad ~~[illegible]~~ praecepta §§ praec. diiudicatur.

Quarum conditionum si una tantum desit A non poterit esse residuum ipsius m. Facile autem ~~videtur~~ perspicietur has conditiones esse sufficientes. Si enim sit

$N \equiv A^2$ mod. a^α
$\equiv B^2$ mod. b^β
$\equiv C^2$ mod. c^γ &c

capiaturque x ita ut sit
$x \equiv \pm A$ mod a^α
$\equiv \pm B$ mod b^β
$\equiv \pm C$ mod c^γ ...

quod fieri potest ob $a, b, c \ldots$ numeros primos diversos (§

~~hic ipsius x~~ x omnibus congruentiis satisfaciet seu erit
$N \equiv xx$ (modd. $a^\alpha, b^\beta, c^\gamma \ldots$) adeoque etiam
$N \equiv xx$ (mod m).

Ad §. 96. & 90.

Ex principiis Cap. praec. illico Criterium desumitur utrum numerus propositus A dati numeri primi p sit residuum an non-residuum. Quum enim residui index debeat esse par $= 2\lambda$, Non-residui vero impar $= 2\lambda+1$; $A^{\frac{p-1}{2}}$ habebit indicem $\lambda(p-1)$, sive $\lambda(p-1) + \frac{1}{2}(p-1)$ prout A est Residuum vel NonResiduum i.e. priori casu $A^{\frac{p-1}{2}} \equiv 1 \pmod p$; posteriori $A^{\frac{p-1}{2}} \equiv -1 \pmod p$ (8 inser)

Ex. Si quaeratur num 3 sit residuum ipsius 13, elevare oportet 3 ad potestatem 6: quoniam vero $3^6 = 729 \equiv 1 \pmod{13}$, 3 erit residuum. ~~Invenitur~~ Estque revera $3 \equiv 4^2$.

Contra $2^6 = 64 \equiv -1$. Quare 2 est non Residuum.

Attamen fatendum est hoc criterium ~~est~~ perraro adhiberi posse quia quando numeri ~~[illegible]~~ examinandi ~~[illegible]~~ aliquantum sunt magni calculi immensi inde nascuntur. Quare maximi momenti est relationem ~~tam~~ aliam simplici~~orem~~ illam ~~quae~~ quam inter modulos residuaque et non residua obtinet omni cura pertractare: ~~quod negotium statim~~ mox aggrediemur. ~~[illegible]~~ Ceterum Criterium hoc § traditam in Cap. 8. ex aliis ~~fonte~~ principiis petitur quae ad congruentias omnes universaliter sese extendunt.

98.

Etsi vero hoc criterium in praxi adhiberi non possit tamen theorema tam elegans quam utile facillime inde deducitur scilicet

Si modulus p fuerit formae $4n+1$: tum -1 erit ipsius residuum

Si vero modulus fuerit formae $4n-1$ tum -1 erit ipsius Non Residuum

Namque priori casu $(-1)^{\frac{p-1}{2}} = (-1)^{2n} = +1$

posteriori vero $(-1)^{\frac{p-1}{2}} = (-1)^{2n-1} = -1$.

Itaque -1 erit residuum numerorum

5. 13. 17. 29. 37. 41. 53. 61. 73. 89. 97 &c

2. 5. 4. 12. 6. 9. 23. 11. 27. 34. 22.

Numeri in serie inferiori sunt radices quadratorum ipsi -1 secundum modulos supra positos congruorum.

Non residuum vero erit -1 numerorum

3. 7. 11. 19. 23. 31. 43. 47. 59. 67. 71. 79. 83. &c.

99.

Sequitur ex § 90. Si a fuerit residuum vel non residuum, -1 autem residuum, tum etiam $-a$ fore vel residuum vel nonresiduum. Sin vero -1 sit non residuum ~~tum~~ $-a$ erit non-residuum priori casu, ~~non~~ residuum posteriori.

Quod itaque est a modulo formae $4n+1$ idem etiam erit $-a$, at pro modulo formae $4n-1$; $-a$ erit contrarium eius quod est $+a$. Hinc apparet numeros usque ad $\frac{p-1}{2}$ tantum examinari oportere utrum sint residua necne: quamobrem ~~in~~ tabella ~~I~~ annexa pro modulis $4n+1$ usque ad hunc terminum est constructa residuisque signum duplex appositum. pro modulis vero $4n-1$ omnium numerorum qui adsunt, complementa ad p desunt.

96.

Quamquam hac demonstratione nil sit simplicius: attamen maximi argumenti erit magisque naturale si ~~hanc~~ haec egregia veritates sine harum principiorum auxilio erui posset quod nunc ut iam § 60 polliciti sumus perficiemus.

~~Si modulum sit~~ infra p ~~4p+1~~ infra ~~hunc numerum~~ p ad p primi erunt ~~4p~~ $p-1$ numeri. ~~Simili autem~~ dem ~~modo~~ ut § 71 ad demonstrationem theor. Celeb. Waring ostendimus, si ex horum numero 1 et $p-1$ ~~excepta~~ excipiantur reliquos ita in classes distribui posse ut quaevis contineat binos numeros diversos quorum productum sit $\equiv +1$. ~~Ex.~~ Harum classium multitudo erit igitur $2n-1$ ~~ex~~ Ex. gr. si p sit $4n+1$; sed ~~multo~~ si $p = 4n-1$ Classes prodibunt $2n-2$; Priori casu igitur classium numerus erit impar, posteriori vero par. Iam facile videtur si habeatur classis a, A tum etiam classem esse $p-a$ et $p-A$ namque $aA \equiv (p-a)(p-A) \pmod p$ i.e. etiam $(p-a)(p-A)$ erit $\equiv 1$. Hinc videtur has classes binarum combinari posse ita $\begin{matrix} a \\ A \end{matrix} \Big| \begin{matrix} p-a \\ p-A \end{matrix} \Big\| \begin{matrix} b \\ B \end{matrix} \Big| \begin{matrix} p-b \\ p-B \end{matrix} \Big\|$ &c

Tales binarum Classium consociationes ~~ad maiorem~~ claritatis caussa ordines vocabimus.

Hinc clarum est: si nulli classi adiuncta est classis ab ipsa non diversa numerum ordinem fore dimidium numeri classium. At pro modulo $p = 4n+1$ Classium numerus est impar. Quare ~~impossibile est~~ fieri nequit ut ordinum numerus sit dimidium numeri classium: necesse est igitur ut unica saltem Classis f, F a socia $p-f, p-F$ non sit diversa. Quum vero ob p primum et imparem f non potest esse $= p-f$, f debet esse $= p-F$ et $F = p-f$. Unde $f^2 = fp - fF$ et $F^2 = Fp - fF$. Hinc tam ff quam $FF \equiv -fF$ at fF per hyp: $\equiv 1$ hinc bina dantur Quadrata $\equiv -1$ Q.E.D.

97.

Exemplo haec demonstratio omnem claritatem adipiscetur. Sit $p = 17$ invenieturque numerorum $2, 3 \ldots. 15$ classes

septem hae: $2,9 \mid 3,6 \mid 4,13 \mid 5,7 \mid 8,15 \mid 10,12 \mid 11,14$

Combinentur harum classium ~~ita ut~~ eae quarum termini sint mutua ad 17 complementa quod ita fiet

$2,9\,;\ 15,8 \mid 3,6\,;\ 14,11 \mid 5,7\,;\ 12,10 \mid$ Relinquitur classis $4, 13$ quae sui ipsius est classis socia estque revera tam 4^2 quam $13^2 \equiv -1$ mod 17.

N° 97

At ~~quatuor~~ talia residua quam aliam valorem +1 et −1 sive p−1 habere nequeunt (quia sunt radices congruentiae secundi gradus $x^2 \equiv 1$), atque +1 necessario est residuum hinc priori casu −1 debet esse residuum posteriori vero nonresiduum Q.E.D.

~~Haecce~~ Haecce etiam demonstratio Illustri Eulero debetur qui et priorem primus inuenit. Exstat in Opusc. Analyticis T. I. p. 135. Quantumuis autem hae duae demonstrationes diuersae esse videntur, propria tamen ex eodem fonte sunt petitae vt peritis patebit postquam hocce argumentum probe penetrauerunt

~~97~~. 101

Postquam igitur criterium nacti sumus ~~et~~ quorum modulorum −1 sit residuum quorumque non residuum pergimus ad residua +2 et −2.

~~Quicunque~~ Si ex tabellas huic operi annexa numeros excerpimus quorum ~~+~~ residuum est +2 hosce habebimus 7, 17, 23, 31, 41 &c. nullusque inter eos numerus occurrit formae $8n+3$ siue $8n+5$. Confirmatur haec inductio si etiam longius progrediamur. ~~Cum vero semper~~ Quod autem et vltra tabulas limites nulli dantur numeri formarum $8n+3$ sive $8n+5$ ~~qui~~ huic legi aduersantes hoc modo facile demonstratur. ⊕ Si tales numeri existerent, ponamus † ita ut ± 2 ~~sit~~ nonresiduum ~~omnium~~ minimum esse ~~s~~ s ~~infra quem igitur~~ vero omnes numeri formarum $8n+3, 8n+5$ ipso s minorum

Habebimus ergo $s=$ ~~Ponamus primo s esse~~ $= 8n+3$. ~~sit~~ atque $\sigma\sigma \equiv 2 \pmod{s}$

† residuum ipsius ~~omnium~~

⊕ Primo obseruare conuenit omnem numerum compositum formae $8n+3$ sive $8n+5$ necessario habere debere factorem sive formae $8n+3$ sive $8n+5$; namque numeri ~~ceterarum~~ reliquarum formarum $8n+1, 8n+7$ quomodocunque inter se multiplicati ~~aliosve~~ tales numeros nullo modo producere possunt.

Si igitur inductio est vera, nullus harum formarum numerus dabitur sive sit compositus sive non, cuius residuum sit 2 ~~certe nullus~~ certe est infra 100 ex inductione nostra. Si vero nihilominus ⊕

Constat pro σ semper binos numeros accipi posse modulo minores qui sibi ipsorum ad hunc modulum sint complementa; adeoque alterum parem alterum imparem. Ponatur ipsius p valor impar eritque $\sigma\sigma - 2 = st$. ~~Iam quum~~ propter σ imparem erit $\sigma\sigma$ ~~formae $8n+1$~~ $\equiv 1 \pmod{8}$ adeoque $\sigma\sigma - 2$ ~~formae $8n-1$~~ $\equiv -1 \bmod 8$

Iam quum. Hinc quum $s \equiv \pm 3$ erit

$-1 \equiv \pm 3t \pmod{8}$ adeoque ~~pro signo superiori~~ $t \equiv \mp 3$.

i.e. t erit etiam formae $8n \pm 3$; ~~erit vero sive primus~~

Iam quum ~~t~~ $\sigma < s$ erit $\sigma\sigma - 2 < ss$ adeoque $\frac{\sigma\sigma - 2}{s} = t < s$

et quia etiam $\sigma\sigma - 2 \equiv 0 \pmod{t}$ sive $\sigma\sigma \equiv 2 \pmod{2}$ i.e. ex suppositione σ esse minimum numerum regulae aduersantem, sequitur eum non esse minimum. Q.E.A.

102.

~~Has igitur~~ Hinc igitur combinando cum praeced. ea quae in § 97 sunt prolata has deduximus veritates

I. Numerorum omnium formae $8n+3$, ~~+~~ $+2$ est Non Residuum.

II. Numerorum omnium primorum formae $8n+3$, -2 est Residuum

III. Numerorum omnium formae $8n+5$, ~~[illegible]~~ $+2$ ~~[illegible]~~ ~~[illegible]~~ est Non Residua.

~~IV. Numerorum omnium primorum formae $8n+5$, -2 est non residuum~~

~~Ultima propositio valet generaliter pro numeris etiam compositis ut statim apparebit.~~

103.

Simili inductione ex tabella inveniuntur numeri primi quorum -2 est non residuum hi: 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71, 79 &c. ita ut -2 sit Non Residuum omnium numerorum primorum formarum $8n+5$, $8n+7$. Observandum est autem ~~[illegible]~~ multiplicatione ex numeris quibuscumque reliquarum formarum $8n+1$, $8n+3$ ~~[illegible]~~ in invicem alios numeros non prodire quam qui similium sint formarum, sive omnis numerus $8n+5$ sive $8n+7$ necessario involvit factorem alterutrius formae, ita ut, saltem intra inductionis limites nullus detur numerus formae ~~aut~~ $8n+5$ aut $8n+7$, neque primus neque compositus cuius Residuum sit -2. Nullos autem huius modi numeros etiam ultra quae igitur eadem erunt cum non residuis ipsius p^n

Quia ergo p^n alia non residua habere nequit nisi quae simul sint non residua ipsius p sequitur .

omnia ipsius p^π residua, simul ipsius p^n i.e cuiuscunque ipsius p potestatis ~~etia~~ residua esse (semper exclusis iis quae p metitur).

95.

Quod autem attinet ad numeros per p divisibiles patet eorum quadrata ~~etiam~~ per p^2 fore divisibilia adeoque ~~nul~~ omnes numeros per p quidem divisibilia non vero per p^2 ipsius p^n (ubi $n > 1$) fore non residua. Generaliter autem si proponatur $p^k A$ ub p ipsum A non metitur hi casus erunt distinguendi

1. Si k sit $=$ sive $> n$ erit $p^k A \equiv 0 \pmod{p^n}$ ideoque residuum,

2. Si k sit $< n$ et impar. ~~Tunc patet~~ Tunc erit $p^k A$ non residuum. Si enim esset $p^k A = p^{2\lambda+1} A \equiv ss$ i.e $p^{2\lambda+1} A - ss$ per p^n ideoque (ob $n \geq 2\lambda+1$) etiam per $p^{2\lambda+1}$ divisibile s necessario per ~~$p^{\lambda+1}$ deberet esse divisibilis~~ esse huius formae $p^{\lambda+1}\sigma$. Tunc vero $p^{2\lambda+1} A - ss$ fit $p^{2\lambda+1}(A - \sigma\sigma p)$. Quia igitur (hyp.) A (per p non dividitur adeoque etiam) $A - ssp$, $p^{2\lambda+1}$ deberet per p^n dividi, minor per maiorem Q.E.A.

3. Si k sit $< n$ et par. Tum erit Ap^k residuum ipsius p^n vel non-residuum prout A fuerit ipsius p residuum vel non residuum.

Namque $Ap^{2\lambda}$ aliter quadrato ss congruum esse nequit nisi (mod p^n) posito $s = p^{\lambda}\sigma$. Ut vero sit $Ap^{2\lambda} \equiv p^{2\lambda}\sigma\sigma$ debet esse $A \equiv \sigma\sigma$ (mod. $p^{n-2\lambda}$) ~~quod est possibile vel~~ i.e. A residuum ipsius $p^{n-2\lambda}$ sive ob A per p indivisibilem residuum ipsius p (§ praec). Unde ~~statim fluit~~ constat assertum.

96.

Judicium de residuis et non-residuis moduli primi potestas qui est numeri reducitur itaque omnino ad casum ubi modulus est numerus primus. Superest casus ubi modulus ~~ubi modulus~~ e numeris primis diversis est compositus. Sit itaque modulus $m = a^{\alpha} b^{\beta} c^{\gamma} \ldots$ ~~Quivis ut N sit resid...~~

$N \equiv xx$ secundum hunc ... secundum singulos factores ... N debet esse residuum tam sing. ~~ipsius~~ ... Quarum conditionum si una ... residuum ipsius m. Facile ... esse sufficientes. Si enim sit

quod ad praecepta §§ praec. diiudicatur.

$N \equiv A^2$ mod. a^{α}
$\equiv B^2$ mod. b^{β}
$\equiv C^2$ mod. c^{γ} &c

capi... $x \equiv$ ... $x \equiv$ ...

~~hic ipsius x~~ x omnibus congruentiis satisfaciet ...

$\therefore N \equiv xx$ (modd. $a^{\alpha}, b^{\beta}, c^{\gamma} \ldots$) ...

$\therefore N \equiv xx$ (mod. m).

Ceterum quivis hanc deductionem attente ponderanti patebit: Cum numeri A, B, C &c. tam positive quam negative accipi possint sive quod idem est tam ipsi numeri ipsi quam eorum complementa ad $a^{\alpha}, b^{\beta}, c^{\gamma}$ &c respective, 2^{μ} diversas combinationes adeoque 2^{μ} diversos ipsius x valores inde oriri si μ sit multitudo factorum $a^{\alpha}, b^{\beta}, c^{\gamma} \ldots$ Fusius ~~de~~ et generalius de hoc argumento in Cap. VIII agetur.

Namque $Ap^{2\lambda}$ aliter quadrato ss congruum esse nequit (mod p^n) nisi posito $s = p^\lambda \sigma$. Ut vero sit $Ap^{2\lambda} \equiv p^{2\lambda}\sigma\sigma$ debet esse $A \equiv \sigma\sigma \pmod{p^{n-2\lambda}}$ ~~[illegible]~~ i.e. A residuum ipsius $p^{n-2\lambda}$ sive ob A per p indivisibilem residuum ipsius p (§ praec). Unde ~~[illegible]~~ constat assertum.

96.

Judicium de residuis et nonresiduis moduli qui est numeri primi potestas reducitur itaque omnino ad casum ubi modulus est numerus primus. Superest casus ubi modulus ubi modulus e numeris primis diversis est compositus. Sit itaque modulus $m = a^\alpha b^\beta c^\gamma \ldots$. ~~A~~ Quum ut ~~A~~ N sit residuum sive ut sit $N \equiv xx$ secundum hunc modulum, haec congruentia etiam secundum singulos factores locum habere debet i.e. N debet esse residuum ~~ipsius~~ tum singulorum modulorum a^α, ~~quam ipsius~~ b^β, c^γ &c. Quarum conditionum si una tantum desit A non poterit esse residuum ipsius m. Facile autem ~~[illegible]~~ perspicietur has conditiones esse sufficientes. Si enim sit

quod ad praecepta §§ praec. diiudicatur.

$$\begin{aligned} N &\equiv A^2 \text{ mod. } a^\alpha \\ &\equiv B^2 \text{ mod. } b^\beta \\ &\equiv C^2 \text{ mod. } c^\gamma \text{ \&c} \end{aligned}$$

capiaturque x ita ut sit

$$\begin{aligned} x &\equiv \pm A \text{ mod } a^\alpha \\ &\equiv \pm B \text{ mod } b^\beta \\ &\equiv \pm C \text{ mod } c^\gamma \\ &\equiv \ldots \end{aligned}$$

quod fieri potest ob $a, b, c \ldots$ numeros primos diversos (§

~~hic ipsius x~~ x omnibus congruentiis satisfaciet seu erit

$N \equiv xx$ (modd. $a^\alpha, b^\beta, c^\gamma \ldots$) adeoque etiam

$N \equiv xx$ (mod m).

97

Ex principiis Cap. praec. illico Criterium desumitur utrum numerus propositus A dati numeri primi p sit residuum an non-residuum. Quum enim residui index debet esse par $= 2\lambda$, Non-residui vero impar $= 2\lambda + 1$; $A^{\frac{p-1}{2}}$ habebit indicem $\lambda(p-1)$, sive $\lambda(p-1) + \frac{1}{2}(p-1)$ prout A est Residuum vel NonResiduum i.e. priori casu $A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$; posteriori $A^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ (8 inser)

Ex. Si quaeratur num 3 sit residuum ipsius 13, elevare oportet 3 ad potestatem 6: quoniam vero $3^6 = 729 \equiv 1 \pmod{13}$, 3 erit residuum. ~~Invenitur~~ Estque revera $3 \equiv 4^2$.

Contra $2^6 = 64 \equiv -1$. Quare 2 est non Residuum.

Attamen fatendum est hoc criterium ~~vix~~ perraro adhiberi posse quia quando numeri ~~paene~~ examinandi ~~[illegible]~~ aliquantum sunt magni calculi immensi inde nascuntur. Quare maximi momenti est relationem aliam ~~tam~~ simpliciter illustrari ~~quae~~ inter modulos residuaque et non residua obtinet quam ~~omni~~ cura pertractare: ~~quod negotium statim~~ mox aggredie-mur. ~~ubi quaedam at~~ Ceterum Criterium hoc § traditum in Cap. 8. ex aliis principiis ~~fonte~~ petitur quae ad congruentias omnes universaliter sese extendunt.

98.

Etsi vero hoc criterium in praxi adhiberi non possit tamen theorema tam elegans quam utile facillime inde deducitur. Scilicet

Si modulus p fuerit formae $4n+1$: tum
-1 erit ipsius residuum
Si vero modulus fuerit formae $4n-1$ tum
-1 erit ipsius Non Residuum

Namque priori casu $(-1)^{\frac{p-1}{2}} = (-1)^{2n} = +1$
posteriori vero $(-1)^{\frac{p-1}{2}} = (-1)^{2n-1} = -1$.

Itaque -1 erit residuum numerorum
5. 13. 17. 29. 37. 41. 53. 61. 73. 89. 97 &c
2. 5. 4. 12. 6. 9. 23. 11. 27. 34. 22.
Numeri in serie inferiori sunt radices quadratorum ipsi -1 secundum modulos supra positos congruorum.

Non residuum vero erit -1 numerorum
3. 7. 11. 19. 23. 31. 43. 47. 59. 67. 71. 79. 83. &c.

99.

Sequitur ex § 90. Si a fuerit residuum vel non residuum, -1 autem residuum, tum etiam $-a$ fore vel residuum vel nonresiduum. Si vero -1 sit non residuum ~~tum~~ $-a$ erit non-residuum priori casu, ~~non~~ residuum posteriori.

Quod itaque est a modulo formae $4n+1$ idem etiam erit $-a$, at pro modulo formae $4n-1$; $-a$ erit contrarium eius quod est $+a$. Hinc apparet numeros usque ad $\frac{p-1}{2}$ tantum examinari oportere utrum sint residua necne: quamobrem ~~in~~ tabella ~~[illegible]~~ annexa pro modulis $4n+1$ usque ad hunc terminum est constructa residuisque signum duplex appositum. pro modulis vero $4n-1$ in omnium numerorum qui adsunt, complementa ad p desunt in

96.

Quamquam hac demonstratione nil sit simplicius: attamen maximi argumenti erit magisque naturale si ~~hanc~~ haec egregia veritates sine harum principiorum auxilio erui possit quod nunc ut iam §60 polliciti sumus perficiemus.

~~Si modulum sit 4p+1~~ infra ~~hunc numerum~~ p ad p primi erunt ~~4p~~ p−1 numeri. ~~Simili autem modo~~ ut §71 ad demonstrationem theor. Celeb. Waring ostendimus, si ex horum numero 1 et p−1 ~~excepta~~ excipiantur reliquos ita in classes distribui posse ut quaevis contineat binos numeros diversos quorum productum sit $\equiv +1$. ~~Ex.~~ Harum classium multitudo erit igitur $2n-1$ ~~Ex. gr.~~ si p sit $4n+1$; sed ~~multitudo~~ si $p=4n-1$ Classes prodibunt $2n-2$; Priori casu igitur classium numerus erit impar, posteriori vero par. Iam facile videtur si habeatur classis a, A tum etiam classem esse p−a et p−A namque $aA \equiv (p-a)(p-A) \pmod p$ i.e. etiam $(p-a)(p-A)$ erit $\equiv 1$. Hinc videtur has classes binarum combinari posse

ita $\begin{matrix} a \\ A \end{matrix} \Big| \begin{matrix} p-a \\ p-A \end{matrix} \Big\| \begin{matrix} b \\ B \end{matrix} \Big| \begin{matrix} p-b \\ p-B \end{matrix} \Big\|$ &c

Tales binarum Classium consociationes ~~ad maiorem~~ claritatis caussa ordines vocabimus.

Hinc clarum est: si nulli classi adiuncta est classis ab ipsa non diversa numerum ordinem fore dimidium numeri classium. At pro modulo $p = 4n+1$ Classium numerus est impar. Quare ~~impossibile est~~ fieri nequit ut ordinum numerus sit dimidium numeri classium: necesse est igitur ut unica saltem Classis ~~f~~ f, F a socia $p-f, p-F$ non sit diversa. Quum vero ob p primum et imparem f non potest esse $= p-f$, f debet esse $= p-F$ et $F = p-f$. Unde $f^2 = fp - fF$ ~~et~~ $F^2 = Fp - fF$. Hinc tam ff quam $FF \equiv -fF$ at fF per hyp: $\equiv 1$ hinc bina dantur Quadrata $\equiv -1$ Q.E.D.

97.

Exemplo haec demonstratio omnem claritatem adipiscetur. Sit $p = 17$ invenieturque numerorum $2, 3 \ldots 15$ classes

septem haec: $2, 9 \mid 3, 6 \mid 4, 13 \mid 5, 7 \mid 8, 15 \mid 10, 12 \mid 11, 14$

Combinentur harum classium ~~ita ut~~ eae quarum termini sint mutua ad 17 complementa quod ita fiet

$2, 9$; $15, 8 \mid 3, 6$; $14, 11 \mid 5, 7$; $12, 10 \mid$ Relinquitur classis $4, 13$ quae sui ipsius est classis socia estque revera tam 4^2 quam $13^2 \equiv -1$ mod 17.

At ~~quatuor~~ talia residua aliam valorem quam +1 et −1 sive $p-1$ habere nequeunt (quia sunt radices congruentiae secundi gradus $x^2 \equiv 1$), atque +1 necessario est residuum hinc priori casu −1 debet esse residuum posteriori vero nonresiduum Q.E.D. N° 97

~~Haecce~~ Haecce etiam demonstratio Illustri ~~Eulero~~ Eulero debetur qui et priorem primus invenit. Exstat in Opusc. Analyticis T. I. p. 135. Quantumvis autem hae duae demonstrationes diversae esse videntur, proprie tamen ex eodem fonte sunt petitae ut peritis patebit postquam ~~hosce~~ argumentum probe penetraverunt

~~97~~. 101

Postquam igitur criterium nacti sumus ~~et~~ quorum modulorum −1 sit residuum quorumque nonresiduum pergimus ad residua +2 et −2.

~~Quicunque~~ Si ex tabella II huic operi annexa numeros excerpimus quorum ~~...~~ residuum est +2 hosce habebimus 7, 17, 23, 31, 41 &c. nullusque inter eos numerus occurrit formae $8n+3$ sive $8n+5$. Confirmatur haec inductio si etiam longius progrediamur. ~~Cum vero semper~~ Quod autem et ultra tabulae limites nulli dantur numeri formarum $8n+3$ sive $8n+5$ ~~qui~~ huic legi adversantes hoc modo facile demonstratur. ⊕ Si tales numeri existerent, ponamus ita ut $+2$ ~~sit~~ nonresiduum minimum esse ~~s~~ s infra ~~quem igitur~~ vero omnes numeri formarum $8n+3$, $8n+5$ ipso s minorum

† residuum ipsius s

omnium

Habebimus ergo $s =$ ~~Ponamus primo s esse~~ $= 8n+3$. atque ~~sit~~ $\sigma\sigma \equiv 2 \pmod{s}$

⊕ Primo observare convenit omnem numerum compositum formae $8n+3$ sive $8n+5$ necessario habere debere factorem sive formae $8n+3$ sive $8n+5$; namque numeri ~~ceterarum~~ reliquarum formarum $8n+1$, $8n+7$ quomodocunque inter se multiplicati ~~alios~~ tales numeros nullo modo producere possunt.

Si igitur inductio est vera, nullus harum formarum numerus dabitur sive sit compositus sive non, cuius residuum sit 2, ~~certe~~ nullus certe est infra 100 ex inductione nostra. Si vero nihilominus ⊕

Constat pro σ semper binos numeros accipi posse modulo minores qui sui ipsorum ad hunc modulum sint complementa; adeoque alterum parem alterum imparem. Ponatur ipsius σ valor impar eritque $\sigma\sigma - 2 = st$. ~~Iam quum~~ propter σ imparem erit $\sigma\sigma$ $\equiv 1 \pmod{8}$ ~~formae 8n+1~~ adeoque $\sigma\sigma - 2$ $\equiv -1 \bmod 8$ ~~formae 8n−1~~

Iam quum. Hinc quum $s \equiv \pm 3$ erit

$-1 \equiv \pm 3t \pmod{8}$ adeoque ~~pro signo superiori~~ $t \equiv \mp 3$,

i.e. t erit etiam formae $8n \pm 3$, ~~erit vero vice primus~~

Iam quum ~~sit~~ $\sigma < s$ erit $\sigma\sigma - 2 < ss$ adeoque $\frac{\sigma\sigma - 2}{s} = t < s$

et quia etiam $\sigma\sigma - 2 \equiv 0 \pmod{t}$ sive $\sigma\sigma \equiv 2 \pmod{2}$ i.e. ex suppositione s esse minimum numerum regulae adversantem, sequitur eum non esse minimum. Q.E.A.

102.

~~Has igitur~~ Hinc igitur combinando cum praeced. ea quae in § 97 sunt prolata has deducimus veritates

I. Numerorum omnium formae $8n+3$, ~~+~~ 2 est Non Residuum.

II. Numerorum omnium primorum formae $8n+3$, -2 est Residuum

III. Numerorum omnium formae $8n+5$, ~~illis~~ $+2$ ~~et~~ -2 ~~sunt~~ est Non Residua.

IV. ~~Numerorum omnium primorum formae $8n+5$, -2 est non residuum~~

~~Atque Ultima propositio valet generaliter pro numeris etiam compositis ut statim apparebit.~~

103.

Simili inductione ex tabella inveniuntur numeri primi quorum -2 est non residuum hi: 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71, 79 &c. ita ut -2 sit Non Residuum omnium numerorum primorum formarum $8n+5$, $8n+7$. Observandum est autem ~~[illegible]~~ multiplicatione ex numeris quibuscunque reliquarum formarum $8n+1$, $8n+3$ ~~[illegible]~~ in invicem alios numeros non prodire quam qui similium sint formarum, sive omnis numerus $8n+5$ sive $8n+7$ necessario involvit factorem alterutrius formae, ita ut, saltem intra inductionis limites nullus detur numerus formae ~~aut~~ $8n+5$ aut $8n+7$, neque primus neque compositus cuius Residuum sit -2. Nullos autem huiusmodi numeros etiam ultra hos limites dari ita demonstramus. Si qui ~~exist~~ exstarent sit omnium minimus ~~ff~~ s infra quem igitur omnium numerorum formarum $8n+5, 8n+7$, -2 sit non residuum, ~~et~~ pro s autem ~~habebit~~ -2 sit residuum. Ponatur $-2 \equiv \sigma\sigma \pmod{s}$ sive $\sigma\sigma + 2 \equiv 0 \pmod{s}$ sumaturque ut in § 101, $\sigma < s$ et impar. erit igitur $\sigma\sigma+2 \equiv 3 \pmod{8}$ quia vero $\sigma\sigma + 2 \equiv 0 \pmod{s}$ i.e. $\sigma\sigma+2 = st$ erit $st \equiv 3 \pmod{8}$ Hinc pro $s = 8n+5$ sive $\equiv 5 \pmod{8}$ erit $5t \equiv 3$ i.e. $t \equiv 7$ sive formae $8n+7$; et pro $s = 8n+7$ sive $\equiv 7$ erit $7t \equiv 3$ i.e. $t \equiv 5$ i.e. formae $8n+5$. At quum $\sigma\sigma+2 = st$ atque $\sigma < s$ facile quisquis videbit t nec maiorem ipso s nec ipsi aequalem esse posse quare $t < s$ i.e. datur infra minimum numerum regulae adversantem adhuc alius Q. E. A.

104.

Hinc simili modo hasce nanciscimur ~~propositiones~~ propositiones:

IV Numerorum omnium formae $8n+5$, -2 est non residuum quod tanquam pro numeris primis styli ex III sequitur ~~complementum theor. 102 III sequi potest~~

V. Numerorum omnium formae $8n+7$ -2 est non residuum

VI. Numerorum omnium primorum formae $8n+\cancel{7}\,3$ -2 est residuum.

Ceterum in utraque demonstratione pro σ etiam numerum parem accipere licuisset: sed tunc iterum distinguendi fuissent casus ubi σ fuisset ~~pariter par~~ sive formae $4n+2$ ab iis ubi $\sigma = 4n$. Evolutio autem ~~omnino~~ perinde procedit ut supra nihilque habet difficultatis.

105

Unicus restat casus scilicet ubi modulus est formae $8n+1$. Hic vero methodum praecedentem prorsus eludit poscitque artificia peculiaria.

Ex principiis cap. praec. sequitur semper dari numeros qui pro ~~tali~~ modulo primo $8n+1$ ad potestatem 8 elevari debent ut unitati fiant congruae: ~~ex~~ horumque numerorum potestatem quartam esse $\equiv -1$. Sit talis numerus f. quare $f^4 \equiv -1 \pmod{8n+1}$ ~~sive~~ quae congruentia ita etiam potest exhiberi $(f^2+1)^2 - 2f^2 \equiv 0 \pmod{8n+1}$ ... (A) sive ita $(f^2-1)^2 + 2f^2 \equiv 0$ ... Ex prima statim sequitur $2f^2$ esse residuum modulo $8n+1$; ex secunda $-2f^2$ etiam esse residuum. Quare quum ~~etiam~~ ff sit ~~resid~~ quadratum atque ~~ergo~~ ipso residuum, erit etiam tam $+2$ quam -2 residuum cujusvis $8n+1$.

106.

Non superfluum erit ostendere quomodo haec theoremata methodo in § 100 ~~ex~~ ~~usurpato~~ adhibito analoge demonstrari possunt unde saltem confirmabitur ambas methodos non esse ita diversas.

Primo tenendum est pro modulo formae ~~[illegible]~~ $4\lambda+1$ ~~esse~~ dari n residua biquadratica diversa. ~~Quamquam hic autem de biqu~~

Facillime quidem hoc ex

principiis Capitis praecedentis derivatur: at periti facile videbunt ~~h~~ hoc theorema etiam independenter ab his principiis demonstrari posse. Quum enim -1 pro tali modulo esse residuum quadraticum demonstraverimus sit $ff \equiv -1$. tunc ~~q~~ clarum est quaternas biquadrata radicum

$+z, -z, +fz, -fz$ omnia inter se congrua

fore adeoque unum tantum residuum biquadraticum praebere Atque facile autem demonstrari potest praeter hos quaternos numeros nullos alios idem praebere. —

<u>Secundo</u> Demonstra~~mus~~ri potest ± 2 semper esse ipsius residuum biquadraticum moduli primi formae $8n+1$, at ~~vero~~ non-residuum modulo $8n+5$. Pro priori enim numerus residuorum biquadraticorum est par pro posteriori impar. At si r est residuum biquadraticum sive $r \equiv z^4$ erit $\frac{1}{r} \equiv \left(\frac{1}{z}\right)^4$ (mod. $8n+1$) adeoque etiam $\frac{1}{r}$ residuum biquadraticum.

Hinc clarum est omnia residua biquadratica ita combinari posse ut quodvis residuum in suum socium multiplicatum fit $\equiv 1$. Reliqua demonstrationis pars ~~de~~monstrationi § 100 omnino est similis ut adeo eam omittere possimus.

<u>Tertio</u> Iam si ~~f ...~~ $f^4 \equiv -1$ (mod $8n+1$) <u>Dico</u> quadratum numeri $f \pm \frac{1}{f}$ (mod $8n+1$) ~~congruum~~ fore $\equiv \mp 2$

Sit enim hoc quadratum $= ff \pm 2 + \frac{1}{ff}$. At ob $f^4 \equiv -1$ erit $ff \equiv \frac{-1}{ff}$ (mod $8n+1$) adeoque Quadratum $\equiv \pm 2$ Q.E.D.

107.

Theoremata haec elegantia tam sagaci Fermatio innotuerunt vid. Op. Mathem. pag: Demonstrationem se habere professus est: nusquam vero eam communicavit. Ab illustri Eulero semper frustra est tentata: At ill. De la Grange primus haec theoremata rigorose demonstravit. Nouveaux Mem de Berlin Année 1775. p . Quod ill. Eulerum adhuc latuisse videtur quando scripsit Diss. in Opusculis. Analyt. conservatam. Vid. T. I. p: 259.

Dimt

108

Progredimur ad residuum 3

Colligendo e tabula omnes modulos quorum non residuum est -3 hosce habebimus: 5, 11, 17, 23, 29, 41, 47, 53 &c. ita ut saltem intra limitem huius inductionis nullus numerus sit numerus primus formae $6n+5$ sive quod eodem redit Exceptomodulo $=2$ formae $3n+2$, cuius -3 sit [redacted] residuum. Quia vero facile videtur ~~nullum~~ quemvis numerum compositum formae $3n+2$ necessario involvere factorem primum eiusdem formae, nullus infra hos limites dabitur numerus formae $3n+2$ cuius -3

sit nonresiduum. Si autem ultra hunc limitem tales numeri darentur sit omnium minimus s ita ut

$s \equiv 2 \pmod{3}$ et $\sigma\sigma \equiv -3 \pmod{s}$ sive ~~$\sigma\sigma + 3 \equiv 0$~~

$\sigma\sigma + 3 \equiv 0 \pmod{s}$ sive $\sigma\sigma + 3 = st$. Iam pro σ dantur bini valores ~~[illegible]~~ $< s$, ~~quorum sumatur~~ qui quum ambo per 3 divisibiles esse nequeunt, sumatur is quem 3 non metitur.

Ergo ob $\sigma\sigma \equiv 1 \pmod{3}$; $s \equiv 2 \pmod{3}$ erit

$1 \equiv 2t \pmod{3}$ sive $t \equiv 2 \pmod{3}$. ~~At ob~~ i.e. t etiam erit formae $3n+2$. Sed propter $\sigma\sigma + 3 = st$ erit -3 etiam residuum ipsius t, et ob $\sigma < s$ facile ~~ei~~ patebit t nec maiorem ipsos nec ipsi aequalem esse posse (unico casu excepto ubi $\sigma = 1$; $s = 2$, $t = 2$ ~~ubi propositio quidem est vera~~ erit. At hunc casum iamiam excepimus) Quamobrem t erit $< s$ i.e. minimus numerus s regulae datae repugnans non est minimus Q.E.A. ios.

Quum numeri formae $3n+2$ sint ipsi qui sunt moduli -3 non residua theorema § praec. demonstratum ita etiam poterit ~~ext~~ efferri.

-3 est non residuum omnium modulorum qui ipsius -3 sunt non residua.

Si itaque tales moduli sint simulque numeri primi ~~el~~ formae $4n+1$, ~~tam~~ i.e. numerorum ~~si sint~~ formae $12n+5$, tam $+3$ quam -3 eorum erit nonresiduum.

Ceterum non ~~[illegible]~~ difficilius cum ipsum casum evolvere ubi σ per 3 ~~[illegible]~~ esset divisibilis tum enim foret $\sigma\sigma+3$ huius formae $9n+3$; t autem hanc haberet formam $3(3n+2)$ i.e. inuol. esset factorum formae $3n+2$. —

II. Si autem sint ~~formae~~ formae $4n-1$; i. e. formae pro numeris primis $12n+11$, -3 erit non residuum hincque $+3$ residuum 0 105

110

Simili modo ex tabula hi invenientur numeri quorum $+3$ est non residuum: ~~13~~ 5, 7, ~~13~~ 17, 19, 29, 31, 41, 43, 53, 67, 79 &c. ita ut ~~omnes~~ numeri primorum formarum $12n+5$ et $12n+7$, $+3$ sit non residuum. Haec inductio vero ob similem rationem ut in § 108 etiam ad numeros compositos se extendit. Demonstratio autem quod etiam extra hunc limitem nulli tales numeri dentur omnino similis est demonstrationibus §§ 101, 103, 108: quare superfluum iudicamus eam hic apponere. Hinc igitur haec sequuntur.

III. ~~Quando numerus est primus et~~ ~~formae~~ $12n+5$ $+3$ est nonresiduum quod pro numeris primis statim ex I sequitur

IV. Numerorum formae $12n+7$, $+3$ est non residuum quare si sint primi -3 erit residuum. ~~Ad adhuc addimus quod~~

111

Nihil autem ex praecedentibus pro numeris formae $12n+1$ sequitur qui adeo artificia singularia requirunt. Ex inductione quidem facile colligitur pro his numeris tam $+3$ quam -3 residua esse: scilicet hoc evenit pro 13, 37, 61, 73, 97, 109 &c. ~~At~

haec inductio eodem modo ~~ad~~ in ~~casus~~ casibus aliquis ~~conforme~~ corroborari nequit. Ceterum si pro talibus numeris primis ~~at~~ modo demonstrari potest -3 esse residuum, eo ipso etiam $+3$ erit residuum. Demonstrabimus autem generaliter -3 esse residuum omnium numerorum primorum formae $3n+1$ quod et eum complectetur casum ubi modulus est formae $12n+7$ pro quo haec proprietas supra est demonstrata.

Ex Cap. praec. sequitur pro modulo formae $3n+1$ semper dari numeros (praeter unitatem) quorum potestas tertia unitati sit congrua. Erit igitur pro tali numero f

$f^3-1\equiv 0 \pmod{3n+1}$ sive

$(f-1)(f^2+f+1)\equiv 0 \pmod{3n+1}$

Quia vero f ab unitate diversus esse supponitur

non erit $f-1\equiv 0$ adeoque oportet esse

$f^2+f+1\equiv 0 \pmod{3n+1}$ hinc erit etiam

$4f^2+4f+4=(2f+1)^2+3\equiv 0 \pmod{3n+1}$

i.e. Datur quadratum ipsi -3 congruum sive -3 est Residuum omnium modulorum primorum formae $3n+1$. Ergo

V. Omnium numerorum primorum formae $12n+1$ ~~tam~~ residuum erit tam $+3$ quam -3.

112.

Teneatur imprimis haec theorematum praecedentium enunciatio:

—3 est Residuum omnium numerorum primorum qui ipsius 3 sunt Residua, Non Residuum vero omnium numerorum qui ipsius 3 sunt Non Residua. Ceterum demonstratio § praec. etiam immutari potuisset instar methodi §§ 100 & 106 usitatae: quod tamen hic omittimus properantes ad magis necessaria. —

Etiam haecce Theoremata apud Fermatium inveniuntur p.

~~Casus §§ 106, 111 considerati ab Ill. Euler iam absoluti~~

Quae de residuis +3 et −3 ~~attinent~~ docuimus iam ab ill. Euler sunt absoluta T. VIII. Comm. Nov. p. 105 sqq. ubi etiam artificium § praec. est adhibitum. Eo magis est memoratu dignum ~~demonstrationem~~ theoremata ad residua +2, −2 pertinentia eius sagacitatem elusisse, quum praecipua difficultas per artificium huic prorsus simile tollatur. Conferantur quae ipse fatetur in hac dissert. p.

— Exstant theoremata etiam demonstrata in diss. Ill. de la Grange d. supra cit: p.

113.

Si ex tabula excerpantur omnes numeri primi quorum +5 est Non Residuum habebuntur hi:

3, 7, 13, 17, 23, 37, 43, 47 etc: Quare saltem ~~per~~ usque ad limitem huius inductionis pro omni ~~modulo~~ numero primo ~~qui est~~ formarum $5n+2$ et $5n+3$ sive qui est non residuum ipsius 5, +5 erit non residuum. Facile vero quisque videbit usque ad limitem huius inductionis assertum etiam ad numeros compositos patere. Ultra hunc limitem nullum numerum (n) ab hac regula excipi sic demonstratur. Si tales numeros dantur sit omnium minimus s ponaturque $\sigma\sigma \equiv 5$ (mod. s) et > 47 sive alio numero ubi igitur s est Non residuum ipsius 5. Erit igitur $\sigma\sigma - 5 = st$.‡ At quum ~~st~~ $\sigma\sigma - 5$ necessario est residuum ipsius 5, s autem est non residuum $\frac{\sigma\sigma - 5}{s} = t$ erit etiam non-residuum ~~ipsius~~ numeri 5. At ex aequatione $\sigma\sigma - 5 = st$ sequitur 5 esse residuum ipsius t, et ~~et σ~~ quia σ ~~semper~~ $< s$ etiam t erit $< s$ i.e. dabitur Nonresiduum ipsius 5, cuius residuum sit 5, minus minimo Non Residuo ipsius 5 hac proprietate praedito Q.E.A. Ceterum ~~si tales~~ si σ ita accipitur ut sit per s divisibilis hic casus non est difficilior ~~tractatu~~ reliquo. ~~Consequitur~~ ~~Quod [illegible]~~ Perinde autem est tractandus ut § 108 docuimus.

(Semper excipitur numerus 2, etiam saepius monuimus)

usque ad quem inductio est continuata

‡ Ubi σ sumi potest $< s$ et per s indivisibilis

114.

~~Demonstratum est autem~~

+5 est ~~res~~ nonresiduum

~~Et~~ Hinc statim sequitur pro omnibus nonresiduis numeri 5 qui sunt ~~huius~~ formae $4n+1$, tam $+5$ quam -5 esse non residuum, pro iis vero qui sunt formae $4n-1$, $+5$ fore non residuum et si sint numeri primi, -5 fore residuum. Priores numeri erant formarum $20n+13, +17$, posteriores vero $20n+3, +7$.

Demonstratur vero methodo huic ~~omnino~~ simili -5 fore non residuum omnium numerorum formarum $20n+11, 13, 17, 19$. quod omittimus quum nullam habeat difficultatem, atque ~~quia~~ quia mox rem maxima generalitate tractabimus. Facile hinc patet $+5$ fore residuum omnium numerorum primorum formarum $20n+11, 19$.

115.

Desunt vero in his ~~numeris~~ formis ~~numeri~~ hae $20n+1, 9$. quae methodum particularem requirunt. Ex inductione statim perspicitur numerorum primorum harum formarum $+5$ esse residuum adeoque et -5. Quod si haec inductio vera est ~~quae~~ combinando cum his praecedentia generalius erit $+5$ residuum omnium numerorum primorum formarum $20n+1$, ~~+~~ $9, 11, 19$ sive quod idem est formarum $5n+1, 4$ i.e. omnium residuorum ipsius 5 (qui sunt numeri primi)

Pro numeris formae $5n+1$ res simili artificio absolvitur ut ante. Namque ex principiis Cap. praec. apparet pro tali modulo semper dari numeros f (ab 1 diversos) ita ut $f^5 \equiv 1 \pmod{5n+1}$. Hinc $f^5 - 1 \equiv 0$ sive
$(f-1)(f^4+f^3+f^2+f+1) \equiv 0$. Quare cum
$f-1$ non sit $\equiv 0$ erit

$$f^4+f^3+f^2+f+1 \equiv 0$$

Hinc quoque

$$4f^4+4f^3+4f^2+4f+4 = (2ff+f+2)^2 - 5f^2$$
$$\equiv 0 \pmod{5n+1}$$

Hinc $5f^2$ erit residuum moduli $5n+1$ ideoque etiam $\frac{5ff}{ff}$ sive $+5$ est residuum cuiusvis numeri primi formae $5n+1$. ~~ideoque ideoque etiam~~

116.

Hoc theorema primum per illustrem De la Grange demonstratum est in dissert. citata ~~le~~, methodusque ab eo adhibita est ~~ab hac~~ a praesenti parum discrepans. Ibidem summus geometra etiam per singularem artificii praeced. modificationem ~~ret~~ id quod adhuc superest demonstravit scilicet esse $+5$ residuum cuiusvis numeri primi formae $5n-1$ sive $5n+4$. De hac re vero infra fusius loquemur. Hic sufficit ex his omnibus colligere theorema sequens

+5 est residuum cuiusvis numeri primi qui est ~~ipsius~~ numeri 5 residuum, nonresiduum vero cuiusvis numeri primi qui numeri 5 est nonresiduum.

Simili modo ut in praecedentibus factum est demonstrari facile poterit
<u>−7 esse non residuum cuiusvis numeri primi qui ipsius 7 est non-residuum.</u>
at ex inductione facile concludi poterit etiam esse
<u>−7 residuum omnium numerorum primorum, qui numeri 7 sunt residua</u>.
Sed hoc a nemine hactenus generaliter est demonstratum. Si quidem numeri forma~~e ips~~ $4n-1$ seorsim considerantur pro his theorema facile demonstratur; opus est scilicet tantum ostendere $+2$ eorum esse non residuum, quod ~~fac~~ fit sine difficultate methodo apagogica sed ~~tale~~ per talem casuum segregationem parum lucramur; quum reliqui hanc methodum semper eludant. Hoc remedio itaque seposito demonstrandum est theorema pro residuis numeri 7 i.e. pro numeris formarum $7n+1$, $7n+2$, $7n+4$. ~~Quod attinet ad primam formam praec~~ Pro prima quidem forma demonstratio ut in praecc. succedit: quum talis expressio $4\cdot\frac{f^7-1}{f-1}$ (ad quam devenire quisquis facile debit qui demonstrationes praecedentes probe penetravit) ita discerpi possit $(2f^3+ff-f-2)^2+7(f^2-f)^2$. — ~~Ceterum~~ hunc ~~casum etiam~~ ill. De la Grange absolvit: at pro reliquis nihil hinc habetur adiumenti. Quare cum tempus

ut aliam viam doceamus. Ceterum infra ~~Art~~ Cap. 6. docebimus

si p sit numerus primus, tum generaliter $\frac{x^p-1}{x-1}$

hoc modo exhiberi posse $X^2 = p\xi^2$ ubi ~~et~~ signum superius pro

$p=4n+1$, inferius pro $p=4n-1$ sumendum est. Quam

X, et ξ autem sunt functiones rationales ipsius x. Hanc

discerptionem ~~sup~~ ultra casum $p=7$ Ill. De la Grange non

perfecit. Capite autem 8 hanc methodum demonstrationi generali

theorematum sequentium adaptabimus.

118

Antequam ulterius progredi possumus propositionem

demonstrare debemus in qua tota demonstrationum sequentium

vis nititur, quaeque quantumvis videatur esse primo aspectu

demonstratu facilis, tamen satis diu nostras meditationes elusit

~~si~~ scilicet

Quemvis numerum non quadratum ~~aliquorum~~ numerorum

esse non residuum. Sufficit vero rem pro numeris primis demonstrare

~~hanc~~ hincque per sequentia facile propositionis veritas generalis

perspicietur.

Facile eius veritas ostenditur si numerus negative sit sumendus. Sit enim ~~primo~~ $= 4n+1$, demonstrandum erit aliquos

dari numeros quorum $-(4n+1)$ sit non residuum

Hoc autem ~~fit~~ evenit pro omnibus numeris huius formae $4aa-4n-1$

Nam $4aa \equiv (4n+1) \bmod (4aa-4n-1)$ adeoque $4n+1$ ~~horum~~ huius modali ~~numerorum~~ erit residuum et quum $4aa-4n-1$ sit formae $4m-1$ -1 erit Non Residuum. Quare $-(4n+1)$ erit Non Residuum **P 113.**

Secundo si proponatur numerus formae $4n-1$ ~~ponatur esse formae $2^n\lambda - 1$ ita ut λ sit impar.~~ Dico quemvis ~~quemcunque~~ $aa+39$ pro numerum formae $4n-1-4aa$ ~~ipsius~~ capiatur $4aa >$ ipsum $-(4n-1)$ fore non residuum modo $4n-1$. Tum enim $4n-1-4aa$ est formae $4m-1$ at ~~$4n-1$ est aa~~ quare -1 erit residuum; ~~quare~~ at $4n-1$ erit $\equiv 4aa$ (mod $4n-1-4aa$) hinc $4n-1$ erit huius moduli residuum adeoque $-(4n-1)$ nonresiduum Q.E.D. Pro unico casu $4n-1=3$ haec demonstratio non valet: at hic nulla demonstratione indiget.

119.

Superest igitur casus ubi signum positive est sumendum. Facile vero res pro numeris formae $4n-1$ absolvitur. ~~Nempe~~ Hic quivis numerus formae $4aa+4n-1$ satisfaciet. Nam quia hoc $-(4n-1) \equiv 4aa$, ($4aa+4n-1$ mod) $-(4n-1)$ erit residuum adeoque quum modulus sit formae $4m+3$, $+(4n-1)$ erit Non Residuum.

Restant igitur numeri formae $4n+1$ qui sunt aut formae $8n+1$, aut $8n+5$. Pro posterioribus etiam demonstratio sine negotio fit. Quivis enim numerus formae $8n+5 \pm 2aa$ satisfaciet. Pro a ~~signo~~ impari superiori hic numerus erit formae $8m+5$ adeoque $\pm 2aa$ eius erit nonresiduum adeoque etiam $8n+5 (\equiv \mp 2aa)$ erit nonresiduum. Pro a im pari $2aa$ hanc habebit formam $8n+2$. Quare pro signo superiori numerus habebit formam $8m+7$ ~~et~~ -2 erit nonresiduum hinc quoque $8n+5$ $(\equiv -2aa)$ erit non Residuum. Pro signo inferiori

numerus erit formae $8m+3$ adeoque $+2$ erit Non Residuum
hinc etiam $8n+5$ $(\equiv 2aa)$ (mod $8m+3$) erit Non Residuum.

120.

Sed casus ubi numerus est formae $8n+1$ artificia tam obvia eludit, methodumque postulat omnino peculiarem. ~~Quae ut omni cura exhibeatur~~ Quam ut omni claritate exhibeamus operam dabimus.
Primo praemittendum est hoc

Theorema. Si habeantur ~~quotcunque~~ duae multitudines numerorum $a, b, c, d \ldots k$ (I); et $A, B, C, D \ldots K$ (II) quae ut eodem terminorum numero constent non est necessarium, eius indolis ut si t sit factor quicunque unius aut plurium terminorum seriei secundae, in serie prima totidem aut plures inveniantur quorum t sit factor: tum dico productum ex terminis omnibus secundae seriei ~~debere esse subm~~ metiri productum ex omnibus terminis primae seriei.

Exemplum sit $12.\,15.\,18 \ldots$ (I) et $3.4.5.6,9.$ (II) eruntque termini divisibiles per
2 in A, B 2; per 3 in AB 3; per 4 in AB 1, per 5 in AB 1; per 6 in B 1 in A 2; per 9 in A, B, 1 at productum ex terminis (I) est 3240 et e terminis (II) etiam 3240

~~in p partes~~ discerpi potest ~~quarum singulae contineant~~ h numeros

facile videtur tum in I dari p numeros $\equiv$ r et in II totidem $\equiv 0$

At si $pm+1 > \mu h$ sed $< (\mu+1)h$, tum inter primos μh terminos in

I, ~~erunt~~ μ erunt $\equiv r$ totidemque in II, $\equiv 0$. ~~At~~ sed in reliquis

post hos μh in I esse potest aut unus terminus $\equiv r$ aut nullus, sed

in II nullus certo datur. Unde constat Propositio.

122

Theorema Sit r ~~forma~~ numerus primus formae $8n+1$.

~~...~~ sit simulque residuum numeri cuiuscunque $h < r$

formetur progressio (I) ....

r, $\frac{1}{2}(r-1)$, $2(r-4)$, $\frac{1}{2}(r-9)$ ... &c. $\frac{1}{2}(r-aa)$ sive $2(r-aa)$

prout a est impar vel par. Tum in serie I totidem termini erunt

per h divisibiles quot sunt in hac II ... 1, 2, 3, ... $2a+1$.

Dem. 1. Si $h = 2$ theorema per se constat tum enim in I omnes

termini praeter primum sunt pares adeoque a termini per 2 divisibiles

Totidem vero sunt in II. vel duplum numeri imparis vel quadruplum

2. Sit h vel numerus ~~aut par~~ impar et $r \equiv \rho\rho \pmod{h}$

tunc in progressione ad minima num III. $-a$, $-(a-1)$, $-(a-2)$ ..... $+a$

totidem termini erunt $\equiv \rho \pmod{h}$ quot sunt in serie II.

$1, 2 \ldots 2a+1$ termini per h divisibiles. At si ~~sit~~ est b terminus

seriei III, $\equiv \rho$ tum erit ~~r−bb~~ terminus correspondens seriei I sive sit

$\frac{1}{2}(r-bb)$ sive $2(r-bb)$ per h divisibilis; nam $r-bb$ est per h divisibilis

& quare quum $\frac{1}{2}(r-bb)$ tunc tantum locum habet quando b est impar sive

formae $8n+1$, $\frac{r-bb}{h}$ certo erit par adeoque etiam
$\frac{\frac{1}{2}(r-bb)}{h}$ numerus integer. De $2(r-bb)$ per se constat.
~~Totidem itaque~~ Quare etiam pro his casibus propositio est demonstrata nisi ~~forte evenire posset ut tam $+b$ quam $-b$ sint $\equiv \varsigma$ adeoque hi duo termini unicum tantum $r-bb$ praebeant~~

3. Sit $\mathfrak{b} \equiv$ ~~numerus formae~~ $8m$, et $bb \equiv r \pmod{8m}$ ....
tum erit etiam vel $bb \equiv r \pmod{16m}$ vel $(b+4m)^2 \equiv r \pmod{16m}$
~~Si igitur Ut certe~~ Quidquid sit ponatur $\varsigma\varsigma \equiv r \pmod{16m}$
eritque etiam $r-bb$ per $16m$ divisibilis quoties
est $\varsigma \equiv b \pmod{8m}$. Sunt vero in serie
$-a$ $-(a-1)$ .... $+a$ ad minimum totidem termini $\equiv \varsigma$
$\pmod{8m}$ quot sunt in hac $1.2.....2a+1$ per $8m$ divisibiles
~~quare~~ unde obtinentur ad minimum totidem valores pro b, sive
totidem termini $r-bb$ ~~seriei I~~ per $16m$ divisibiles quot sunt
in serie III per $8m$ divisibiles. ~~Jam quum sint termini~~ Quamobrem
quum ~~in~~ seriei I ~~totidem~~ termini sint aut $\frac{1}{2}(r-bb)$ aut $2(r-bb)$ erunt in hac
serie ad minimum totidem termini per $8m$ divisibiles quot sunt in
III. Q.E.D.

4. Ne demonstratio interrumperetur tacite in 2 et 3 ~~affirm~~ supposuimus
cuivis ~~cuius~~ valorem ~~dare~~ b correspondere termino peculiari $r-bb$ sive ~~proprio~~ quod
esset falsum si evenire posset ut tam $-b$ quam $+b \equiv \varsigma$

formae $8n+1$, $\frac{r-bb}{h}$ certo erit par adeoque etiam

$\frac{\frac{1}{2}(r-bb)}{h}$ numerus integer. De $2(r-bb)$ per se constat.

~~Totidem itaque~~ Quare etiam pro his casibus propositio est demonstrata nisi ~~forte evenire possit ut tam $+b$ quam $-b$ sint $\equiv \varsigma$ adeoque hi duo termini unicum tantum $r-bb$ praebeant.~~

3. Sit h ~~numerus formae~~ $= 8m$, et $bb \equiv r \pmod{8m}$ ....

tum erit etiam vel $bb \equiv r \pmod{16m}$ vel $(b+4m)^2 \equiv r \pmod{16m}$

~~Si igitur Ut certo~~ Quidquid sit ponatur $\varsigma^2 \equiv r \pmod{16m}$

eritque etiam $r-bb$ per $16m$ divisibilis ~~si~~ quoties

est $\varsigma \equiv b \pmod{8m}$. Sunt vero in serie

$-a$, $-(a-1)$ .... $+a$ ad minimum totidem termini $\equiv \varsigma$

(mod. $8m$) quot sunt in hac $1.2 \ldots 2a+1$ per $8m$ divisibiles

~~quare~~ unde obtinentur ad minimum totidem valores pro b, sive

totidem termini $r-bb$ ~~seriei I~~ per $16m$ divisibiles quot sunt

in serie III per $8m$ divisibiles. ~~Quum quum sint termini~~ Quamobrem

quum ~~in~~ seriei I ~~totidem~~ termini sint aut $\frac{1}{2}(r-bb)$ aut $2(r-bb)$ erunt in hac

serie ad minimum totidem termini per $8m$ divisibiles quot sunt in

III. Q.E.D.

4. Ne demonstratio interrupperetur tacite in 2 et 3 ~~assum~~ supposuimus

quemvis ~~ipsius~~ b valorem ~~dare~~ correspondere termino peculiari $r-bb$ sive ~~proprio~~ quod

esset falsum si evenire posset ut tam $-b$ quam $+b \equiv \varsigma$

4 33

E

Caput tertium.

De Residuis functionum exponentialium.

39

Th. Si $a^m \equiv \mu$, $a^n \equiv \nu$, $a^p \equiv \pi$, &c erit $a^{m+n+p\ldots\ldots} \equiv \mu\nu\pi\ldots\ldots$ secundum eundem modulum ~~atque~~ ac proinde etiam $a^{tm} \equiv \mu^t$.

Demonstratio continetur ~~in~~ §. 11.

40.

Theor Si $a^m \equiv \mu$, $a^n \equiv \nu$, secundum modulum qui sit primus, a non metiens ~~erit a^m~~ atque $m > n$ erit $a^{m-n} \equiv \frac{\mu}{\nu}$

Vid. §. . — In §§ sequentibus (usque ad § 74) semper intelligendum est modulum assumi qui sit numerus primus, numerumque a non metiatur

41.

Theor. In serie geometrica $1, a, aa, a^3\ldots\ldots$ certo occurret terminus a^t qui sit $\equiv 1$ secundum modulum p, ~~primum~~, ~~ipsum a non metientem,~~ ~~et~~ quidem ita ut sit $t < p$.

Demonstr. Si omnium terminorum secundum p residua minima positiva eruantur, alia non prodibunt atque

1, 2, 3 .... $p-1$ quorum numerus $= p-1$. Igitur necesse est ut inter terminos $1, a, \ldots\, a^{p-1}$ ~~duo ad minimum repe-riantur~~ quorum multitudo $= p$, duo ad minimum inveniantur qui idem residuum praebeant. Sint hi a^m, a^n sitque $m > n$, eritque ex § praec. $a^{m-n} \equiv 1$; manifestoque erit $m-n < p$. Q. E. D.

Exempl. Si progressioni 1, 2, 4, 8 &c. modulus ~~17~~ 13 adaptetur invenitur ~~[illegible]~~ $2^{12} (= 4096) \equiv 1$. At secundum modulum 23 iam erit $2^{11} (= 2048) \equiv 1$. Simili modo numeri 5 potestas sexta, 15625, ~~secun~~ invenitur unitati congrua secundum 7; ~~at secundum~~ quinta contra 3125 secundum 11. Videmus itaque in aliis casibus ad potestatem $p-1$ tam ascendere nos debere, in aliis potestatem inferiorem sufficere.

42.

Si progressio ultra terminum qui unitati est congruus continuetur, eadem residua rursus eruentur quae ab initio prodierant; Scilicet si $a^t \equiv 1$, erit $a^{t+1} \equiv a$, $a^{t+2} \equiv aa$ &c., donec post t terminos ad a^{2t} perveniatur, quae ~~est~~ iterum unitati est congruus atque seriem residuorum primam denuo inchoat. Habetur itaque periodus t residua continens, quae simulac finita est semper ab initio repetitur, ~~[illegible]~~ aliaque evolui nequeant nisi qui in hac periodo sint comprehensa.

‡ $a^{mt} \equiv 1$ et

In genere erit ‡ $a^{mt+n} \equiv a^n$ haecque proprietas secundum nostram designandi methodum ita poterit exhiberi.

$$\text{Si } \cancel{t}\ \cancel{m}^{\,r} \equiv \cancel{p}^{\,\varrho} \pmod{t}$$

$$\text{erit } a^r \equiv a^\varrho \pmod{p}$$

43.

Ista veritas administrat compendium perutile ad residua potestatum ~~invenienda~~ ex, ~~quo~~ exponente quantumvis magno affectarum, expedite invenienda, simulac potestas innotescit quae unitati est congrua. Ex. gr. quaeratur residuum ex divisione potestatis 3^{1000} per 13 oriundum. Quoniam $3^3 \equiv 1 \pmod{13}$ erit $t \equiv 3$, ~~quumque secundum~~ [illegible] et quum

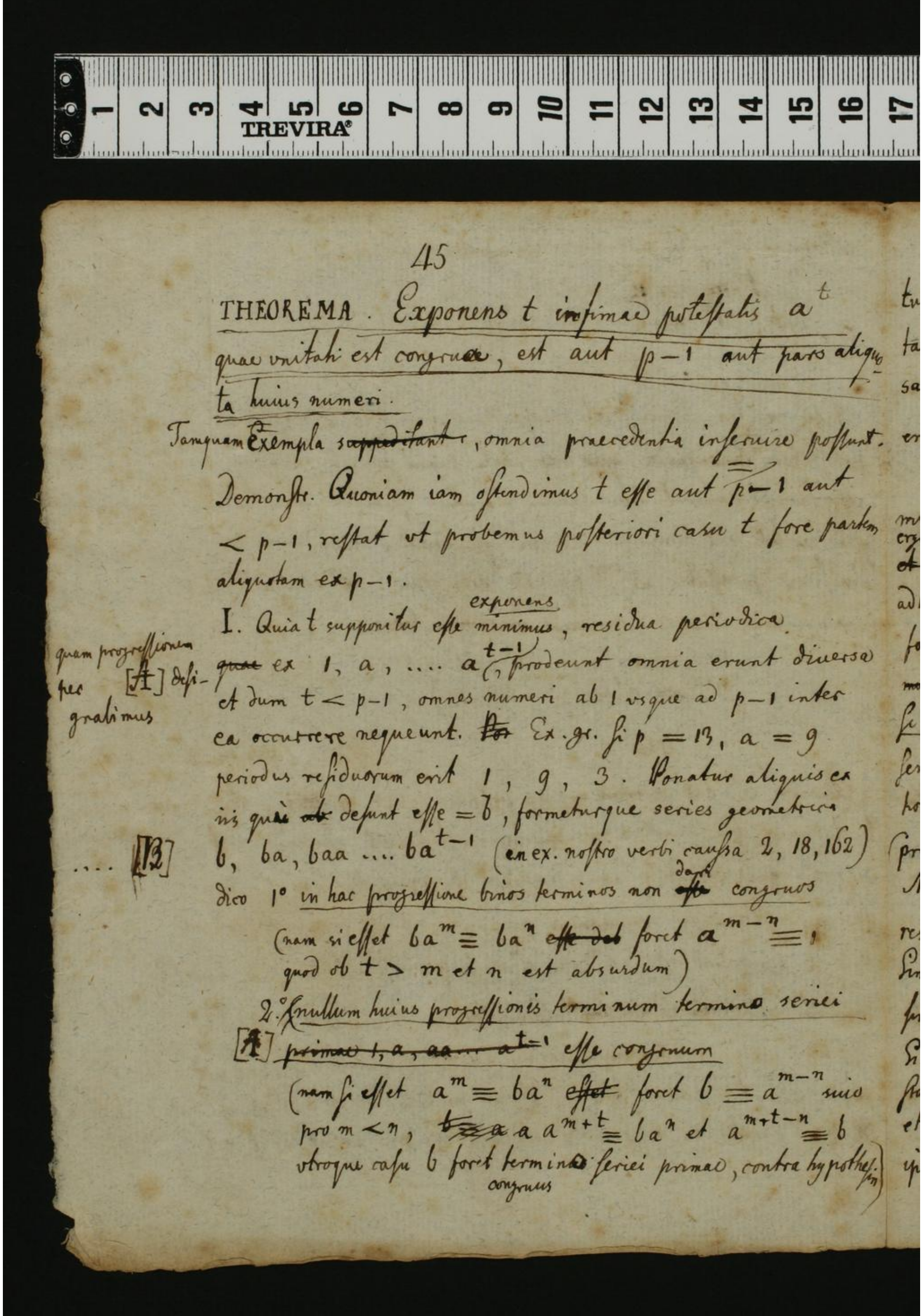
$$1000 \equiv 1 \pmod{3} \text{ erit}$$

$$3^{1000} \equiv 3^1 (= 3) \pmod{13}.$$

44

Quando a^t est ~~minima~~ infima potestas, quae est $\equiv 1$, illi t termini qui periodum residuorum constituunt omnes erunt diversi, quod ex indole demonstrationis §. 41 nullo negotio perspicitur. (praeter $a^0 = 1$ quod per se clarum) ad quem casum hic non respicimus. Hoc casu ~~congruentia~~ propositio §. 42 converti poterit Scilicet non potest esse $a^m \equiv a^n \pmod{p}$ nisi sit $m \equiv n \pmod{t}$

~~Sit enim residua [illegible] ipsorum [illegible]~~ sint Si enim haec conditio deficeat, residua minima ipsorum m, n secundum t, quae sint μ, ν, erunt diversa (§ 6). Verum ex §. 42 erit $a^\mu \equiv a^\nu$, ubi μ, et ν sunt $< t$ ~~[illegible]~~ quod propter ea quae modo diximus esse non potest, si t est exponens minimus.



45

THEOREMA. Exponens t infimae potestatis a^t quae unitati est congrua, est aut $p-1$ aut pars aliquota huius numeri.

Tanquam Exempla ~~suppeditant~~, omnia praecedentia inservire possunt.

Demonstr. Quoniam iam ostendimus t esse aut $= p-1$ aut $< p-1$, restat ut probemus posteriori casu t fore partem aliquotam ex $p-1$.

I. Quia t supponitur esse exponens minimus, residua periodica ~~quae~~ ex $1, a, \ldots a^{t-1}$ prodeunt omnia erunt diversa et dum $t < p-1$, omnes numeri ab 1 usque ad $p-1$ inter ea occurrere nequeunt. ~~Ex~~ Ex. gr. si $p = 13$, $a = 9$ periodus residuorum erit 1, 9, 3. Ponatur aliquis ex iis qui ~~ab~~ desunt esse $= b$, formeturque series geometrica $b, ba, baa \ldots ba^{t-1}$ (in ex. nostro verbi caussa 2, 18, 162) .... [B]

quam progressionem per [A] designatimus

dico 1° in hac progressione binos terminos non ~~esse~~ dari congruos

(nam si esset $ba^m \equiv ba^n$ ~~esse deb~~ foret $a^{m-n} \equiv 1$, quod ob $t > m$ et n est absurdum)

2.° nullum huius progressionis terminum termino seriei [A] ~~primae $1, a, aa \ldots a^{t-1}$~~ esse congruum

(nam si esset $a^m \equiv ba^n$ ~~esset~~ foret $b \equiv a^{m-n}$ sive pro $m < n$, ~~$b \equiv a$~~ $a\, a^{m+t} \equiv ba^n$ et $a^{m+t-n} \equiv b$ utroque casu b foret terminus congruus seriei primae, contra hypothesin)

Si itaque residua minima ~~eruantur~~ progressionis b, ~~ba, baa ... ba~~$^{t-1}$ (B) eruantur ~~habebuntur~~ quorum multitudo erit $= t$, hae omnia tam inter se quam a residuis ex serie (A) oriundis erunt diversa. Habentur itaque iam $2t$ residua diversa. In ex. nostro erunt 1, 9, 3 ; 2, 5, 6. 6

~~Ergo~~ Si nunc hae $2t$ residua omnem residuorum possibilium multitudinem exhauriant esse debet $2t = p-1$ et $t = \frac{1}{2}(p-1)$ ~~et~~ ergo theorema nostrum erit demonstratum. Sin minus, ponamus deesse adhuc quaedam residua ex quorum numero sit c (nostro casu ex. gr. 4) formeturque progressio tertia $c, ca, caa, \ldots\ ca^{t-1} \ldots (C)$. Demonstratur ~~mox~~ simili modo ut antea 1°. ~~nullum~~ non dari binos huius seriei terminos ~~...~~ inter se congruos. 2°. nullum huius seriei terminum esse congruum termino serierum (A) et (B). Prima assertio probatur ut antea, ~~secund~~ posterior hoc modo. Si esset $ca^m \equiv ba^n$, foret $c \equiv ba^{n-m}$ sive $\equiv ba^{t+n-m}$ (prout $n >$ sive $< m$) i.e. utroque casu ~~congruus~~ $\equiv$ termino seriei B.

Nancissimur itaque hoc modo $3t$ residua diversa, quae si omnem residuorum possibilium numerum expleant erit $t = \frac{1}{3}(p-1)$.

Sin minus progrediendum est ad seriem quartam ~~de~~ qua prorsus simili modo demonstratur, quod t nova residua inde obtineantur.

Si hoc modo pergamus donec multitudo omnium numerorum exhausta erit, inveniemus illam esse aut t, aut $2t$ aut $3t$ aut $4t$ etc. i.e. multiplum ipsius t atque proin t erit pars aliquota ipsius $p-1$. Q. E. D.

In nostro exemplo series hae ita inveniuntur

(A) ... 1 . 9 . 3
(B) .... 2 . 5 . 6
(C) ..... 4 . 10 . 12
(D) .... 7 . 11 . 8

et erit t (i.e. 3) quarta pars ipsius $p-1$ (i.e 12)

46.

Quia constat $p-1$ semper esse multiplum ~~ipsius~~ exponentis minimae potestatis unitati congruae, sequitur potestatem (~~p − 1) tam~~ cuius exponens est $p-1$, unitati semper fore congruam, sive $a^{p-1}-1$ per p semper erit divisibilis si p est primus ipsum a non metiens.

Theorema hoc peregregium cui magna pars eorum quae in hoc genere ulterius sunt inventa innititur ab inventore Theorema Fermatianum appellari solet. Vid. ~~D.~~ Fermatii ~~quamquam ......~~ ~~qui a quo~~ ~~Opusculum~~ Opera mathematica Tolosae 1679 fol. p. . Demonstrationem inventor non adiecit, ~~quamquam~~ attamen eam in potestate esse professus est. Ill. Euler ~~qui ...~~ ~~numerorum theoriam excolere coepit~~ primus publicavit demonstrationem a. in ~~com~~ commentatione, „ Comment. Acad. Petrop. *) . Innititur ea evolutioni

---

* in Dissert. anteriore videmus virum summum ad scopum nondum pervenisse.

7

potestatis $(a+1)^p$ ~~(a+1)~~ ex qua sequitur
$(a+1)^p-(a+1)$ per p fore divisibilem, si a^p-a fuerit divisibilis, ut cuique tentanti facile illucescet. Jam quia
1^p-1 per p est divisibilis erit etiam 2^p-2. hinc 3^p-3 et
~~sic porro~~ &c. et in genere a^p-a (ubi semper p supponitur esse
numerus primus). Si itaque a per p non dividitur erit
$\frac{a^p-a}{a}$ ~~per~~ i.e. $a^{p-1}-1$ per p divisibilis. — Sufficiet hoc ad
methodi indolem declarandam, – Clar. Lambert dedit quoque
theorematis demonstrationem in Actis Helveticis
et Actis Erud. 1769. p
ab Euleriana prima parum discrepantem. — At quia binomii
evolutio a numerorum theoria prorsus est aliena Ill. Euler
operam dedit ad aliam inveniendam quae exstat
~~[illegible]~~. Haec sola genuina esse videtur, haecque
quam nos dedimus prorsus cum ea convenit. ~~verisimile est~~ ~~[illegible]~~ demon-
~~strationem Fermatianam eandem fuisse~~, quum quia calculus literalis
tunc temporis nondum erat satis excultus *), tum quia Vir sagacissimus
theorema tam generaliter ut est in § praec. proposuit, ad quem finem
methodus analyticus per multas demum ambages

* Quamquam Fermatius Theorema binomiale novisse videtur, de qua re forsan
alia occasione opinionem dicemus

47.

Quia itaque exponens infimae potestatis numeri cuiusuis, vnitati congruae est vnus e factoribus numeri $p-1$, omnes numeri secundum hunc factorem classificari poterunt, ita vt numeri ~~orum~~ factori alioni adscripti ~~orum~~, ad hanc potestatem euecti, vnitati sint congrui, ad potestatem ~~omnes~~ vero ~~potestates~~ hac inferiorem incongrui. Sufficit autem numeros tantum positiuos modulo minores considerauisse; nam quoniam ~~ceteri~~ omnis alius horum alioni debet esse congruus, ~~ad fut~~ ad eundem exponentem referendus est; ~~quod~~ ~~[illegible]~~ propter congruentiam potestatum similium, numerorum congruorum. Ex. gr. pro ~~mod~~ $p = 19$, numeri ab 1 vsque ad 18 ita sunt ~~diver~~ distribuendae inter factores numeri 19.

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

Inuestigatio accurata, quot ad quemque exponentem pertineant numeri ad quam statim progredimur maximi est momenti.