et non-diuisorum exstare *), vnde non difficile erat *quales* esse debeant deriuare: methodus autem qua vsus est ad comprobationem illius suppositionis haud idonea videtur. In alio schediasmate, *De criteriis aequationis* $fxx + gyy = hzz$ *vtrumque resolutionem admittat necne*, *Opusc. Anal. T. I.* (vbi f, g, h sunt dati, x, y, z indeterminati) per inductionem inuenit, si aequatio pro aliquo valore ipsius $h = s$ solubilis sit, eandem pro quouis alio valore ipsi s secundum mod. $4fg$ congruo, siquidem sit numerus primus, solubilem fore, ex qua propositione suppositio de qua diximus haud difficile demonstrari potest. Sed etiam huius theorematis demonstratio omnes ipsius labores elusit **), quod non est mirandum, quia nostro iudicio a theoremate fundamentali erat proficiscendum. Ceterum veritas huius propositionis ex iis quae in sect. sequenti docebimus sponte demanabit.

Post Eulerum, clar. Le Gendre eidem argumento operam nauauit, in egregia tract. *Re-*

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

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

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

152. Hactenus congruentiam puram $xx \equiv A \pmod{m}$ tractauimus, ipsiusque resolubilitatem dignoscere docuimus. *Radicum ipsarum*

inuestigatio per art. 105 ad eum casum est reducta, vbi m est aut primus aut primi potestas, posterior vero per art. 101 ad eum vbi m est primus. Pro hoc autem casu ea quae in art. 61 *sqq* tradidimus vna cum iis quae in sect. V et VIII docebimus, omnia fere complectuntur quae per mothodos directas erui possunt. Sed hae vbi sunt applicabiles plerumque infinities prolixiores sunt quam indirectae quas in sect. VI. docebimus, adeoque non tam propter vtilitatem suam in praxi quam propter pulcritudinem memorabiles. — *Congruentiae secundi gradus non purae* ad puras facile reduci possunt. Proposita congruentia $axx + bx + c \equiv o$ secundum mod. m soluenda, huic aequiualebit congruentia $4aaxx + 4abx + 4ac \equiv o$ (mod. $4am$), i. e. quiuis numerus alteri satisfaciens etiam alteri satisfaciet. Haec vero ita exhiberi potest $(2ax + b)^2 \equiv bb - 4ac$ (mod. $4am$), vnde omnes valores ipsius $2ax+b$ minores quam $4am$ si qui dantur inueniri possunt. Quibus per r, r', r'' etc. designatis, omnes solutiones congr. prop. deducentur ex solutionibus congruentiarum $2ax \equiv r - b$, $2ax \equiv r' - b$ etc (mod. $4am$) etc., quas in sect. II inuenire docuimus. Ceterum obseruamus, solutionem plerumque per varia artificia contrahi posse, ex gr. loco congr. prop. aliam inueniri posse $a'xx + 2b'x + c' \equiv o$, illi aequipollentem, et in qua a' ipsum m metiatur; haec vero de quibus Sect. vltima conferri potest, hic explicare breuitas non permittit.