$4m - 1$, *tale quadratum non datur*, hoc modo demonstratum est ab ill. Eulero, *Comm. nou. Acad. Petrop.* T. XVIII. p. 112 ad annum 1773. Demonstrationem aliam iam multo ante dederat, *Comm. nou.* T. V. p. 5 qui prodiit a. 1760. In dissert. priori, Comm. nou. T. IV, p. 25, rem nondum perfecerat. Postea etiam ill. La Grange theorematis demonstrationem tradidit, Nouveaux Mem. de l'Ac. de Berlin A. 1775 p. 342. Aliam adhuc demonstrationem in sectione sequenti vbi proprie de hoc argumento agendum erit, dabimus.

65. Postquam omnes expressiones $\sqrt[n]{A}$ (mod. p) ad tales reducere docuimus, vbi n diuisor numeri $p-1$, criteriumque nacti sumus vtrum valores reales admittat, necne, tales expressiones $\sqrt[n]{A}$ (mod. p) vbi n ipsius $p-1$ est diuisor accuratius considerabimus. Primo ostendemus, quam relationem valores singuli expressionis inter se habeant, tum artificia quaedam trademus, quorum auxilio vnus valor expressionis saepenumero inueniri possit.

Primo, quando $A \equiv 1$, atque r aliquis ex n valoribus expressionis $\sqrt[n]{1}$ (mod. p), siue $r^n \equiv 1$ (mod. p), omnes etiam ipsius r potestates erunt valores istius expressionis; horum autem totidem erunt diuersi quot vnitates habet exponens ad quem r pertinet (art. 48). Quodsi igitur r est valor ad exponentem n pertinens, potestates ipsius r hae $r, r^2, r^3 \ldots r^n$ (vbi loco vltimae *vnitas* substitui potest) omnes expressionis $\sqrt[n]{1}$ (mod. p) valores inuoluent. Qualia

autem subsidia exstent ad tales valores inueniendos qui ad exponentem n pertineant, in sect. VIII fusius explicabimus.

Secundo. Quando A vnitati est incongruus, vnusque expressionis $\sqrt[n]{A}$ (mod. p) notus, qui sit x, reliqui hoc modo inde deducuntur. Sint valores expressionis $\sqrt[n]{1}$, r, $r^2 \ldots r^{n-1}$ (vti modo ostendimus), eruntque omnes expr. $\sqrt[n]{A}$ valores hi: x, xr, $xr^2 \ldots xr^{n-1}$; namque omnes hos congruentiae $x^n \equiv A$ satisfacere inde manifestum quod, posito quocunque eorum $\equiv xr^k$ potestas ipsius n^{ta}, $x^n r^{nk}$, propter $r^n \equiv 1$ et $x^n \equiv A$, vnitati fit congrua: omnes diuersos esse ex art. 23 facile intelligitur; plures autem valores quam hos quorum numerus est n, expressio $\sqrt[n]{A}$ habere nequit. Ita ex. gr. si alter expressionis $\sqrt[2]{A}$ valor est x, alter erit $-x$. Denique hinc concludendum omnes valores expr. $\sqrt[n]{A}$ inuenire non posse, nisi simul omnes valores expr. $\sqrt[n]{1}$ constent.

66. Secundum quod nobis proposueramus fuit, docere, in quo casu vnus expressionis $\sqrt[n]{A}$ (mod. p) valor (vbi n supponitur esse diuisor ipsius $p-1$) directe inueniri possit. Hoc euenit quando aliquis valor potestati alicui ipsius A congruus euadit, qui casus quum haud raro occurrat, aliquantum huic rei immorari non superfluum erit. Sit talis valor, *si quis datur* x, siue $x \equiv A^k$ et $A \equiv x^n$ (mod. p). Hinc colligitur $A \equiv A^{kn}$; quare si numerus k habetur, ita vt sit $A \equiv A^{kn}$, A^k erit valor quaesitus. At huic conditioni aequiualet ista, vt sit $1 \equiv kn$ (mod. t),

designante t exponentem ad quem pertinet A (art. 46, 48). Vt vero haec congruentia possibilis sit, requiritur, vt sit n ad t primus. Hoc in casu erit $k \equiv \frac{1}{n} \pmod{t}$; si vero t et n diuisorem communem habent, nullus valor x potestati ipsius A congruus esse potest.

67. Quum autem ad hanc solutionem ipsum t nouisse oporteat, videamus quomodo procedere possimus, si hunc numerum ignoremus. Primo facile intelligitur, t ipsum $\frac{p-1}{n}$ metiri debere, siquidem $\sqrt[n]{A} \pmod{p}$ valores reales habeat, vti hic semper supponimus. Sit enim quicunque valor y, eritque tum $y^{p-1} \equiv 1$, tum $y^n \equiv A \pmod{p}$; quare eleuando partes posterioris congruentiae ad potestatem $\frac{p-1}{n}$ tam, fiet $A^{\frac{p-1}{n}} \equiv 1$; adeoque $\frac{p-1}{n}$ per t diuisibilis (art 48). Iam si $\frac{p-1}{n}$ ad n est primus, congruentia art. praec. $kn \equiv 1$ etiam secundum modulum $\frac{p-1}{n}$ solui poterit, manifestoque valor ipsius k congruentiae secundum modulum hunc satisfaciens eidem etiam secundum modulum t, qui ipsum $\frac{p-1}{n}$ metitur, satisfaciet, (art. 5). Tum igitur quod quaerebatur inuentum. Si vero $\frac{p-1}{n}$ ad n non est primus, omnes ipsius $\frac{p-1}{n}$ factores primi qui simul ipsum n metiuntur ex $\frac{p-1}{n}$ eiiciantur. Hinc nanciscemur numerum $\frac{p-1}{nq}$, ad n primum, designante q productum ex omnibus illis factoribus primis, quos eiecimus. Quodsi iam conditio ad quam in artic. praec. peruenimus vt t ad n sit primus locum habet, t etiam ad q erit primus adeoque etiam ipsum $\frac{p-1}{nq}$ metietur. Quare si congruen-