II. Per formam $xx + 2yy$ nullus numerus, cuius non-residuum -2, ita repraesentari potest vt x ad y sit primus, reliqui omnes poterunt. Sit -2 residuum numeri M, atque N valor aliquis expr. $\sqrt{-2}$ (mod. M). Tum per art. 176 formae $(1, 0, 2)$, $(M, N, \frac{NN+2}{M})$ proprie aequiualentes erunt. Transeat illa proprie in hanc ponendo $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, eritque $x = \alpha$, $y = \gamma$ repraesentatio numeri M ad N pertinens. Praeter quam et hanc $x = -\alpha$, $y = -\gamma$ aliae ad N non pertinebunt (art. 180).

Simili modo, vt supra, perspicitur, repraesentationes $x = \pm\alpha$, $y = \mp\gamma$ ad valorem $-N$ pertinere. Omnes vero hae quatuor repraesentationes vnicam tantum discerptionem ipsius M in quadratum et quadratum duplex exhibent, et si praeter N et $-N$ alii valores expr. $\sqrt{-2}$ (mod. M) non dantur, aliae discerptiones non dabuntur. Hinc adiumento proposs. art. 116 facile deducitur theorema:

quiuis numerus positiuus reduci potest, faciendo $\mu = 0$ quando M est impar, et $S = 1$ quando M nullos factores formae $4n + 3$ implicat): M *nullo modo* in duo quadrata resolui poterit, si S est non-quadratus; si vero S est quadratus, dabuntur $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. discerptiones ipsius M, quando aliquis numerorum α, β, γ etc. est impar, aut $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. $+ \frac{1}{2}$, quando omnes α, β, γ etc. sunt pares (siquidem ad quadrata ipsa tantum respicitur). Qui in calculo combinationum aliquantum sunt versati, demonstrationem huius theorematis (cui, perinde vt aliis *particularibus*, immorari nobis non licet) ex theoria nostra generali haud difficulter eruere poterunt. Cf. art. 105.

Quiuis numerus primus formae $8n + 1$ *vel* $8n + 3$ *in quadratum et quadratum duplex decomponi potest et quidem vnico tantum modo.* $1 = 1 + 0$, $3 = 1 + 2$, $11 = 9 + 2$, $17 = 9 + 8$, $19 = 1 + 18$, $41 = 9 + 32$, $43 = 25 + 18$, $59 = 9 + 50$, $67 = 49 + 18$, $73 = 1 + 72$, $83 = 81 + 2$, $89 = 81 + 8$, $97 = 25 + 72$ etc.

Etiam hoc theorema, vti plura similia, Fermatio innotuit: sed ill. La Grange primus demonstrationem dedit, *Suite des recherches d'Arithmetique, Nouv. Mem. de l'Ac. de Berlin* 1775, *p.* 323 *sqq.* Multa ad idem argumentum pertinentia iam ill. Euler absoluerat, *Specimen de vsu obseruationum in mathesi pura Comm. nou. Petr. T. VI p.* 185 *sqq.* Sed demonstratio completa theorematis semper ipsius industriam elusit, p. 220. Conf. etiam diss. in T. VIII (ad annos 1760, 1761), *Supplementum quorundam theorematum arithmeticorum*, sub fin.

III. Per methodum similem demonstratur, quemuis numerum cuius residuum quadr. sit -3 repraesentari posse aut per formam $xx + 3yy$, aut per hanc $2xx + 2xy + 2yy$, ita vt valor ipsius x ad valorem ipsius y sit primus. Quare quum -3 sit residuum omnium numerorum primorum formae $3n + 1$ (art. 119) manifestoque per formam $2xx + 2xy + 2yy$ numeri *pares* tantum repraesentari possint: eodem modo vt supra habetur theorema:

Quiuis numerus primus formae $3n + 1$ in quadratum et quadratum triplex decomponi potest, et quidem unico tantum modo. $1 = 1 + 0$, $7 = 4 + 3$, $13 = 1 + 12$, $19 = 16 + 3$, $31 = 4 + 27$, $37 = 25 + 12$, $43 = 16 + 27$, $61 = 49 + 12$, $67 = 64 + 3$, $73 = 1 + 72$ etc.

Demonstrationem huius theorematis ill. Euler primus tradidit in commentatione modo laudata, *Comm. nou. Petr. T. VIII*, *p.* 105 *sqq.*

Simili modo vlterius progredi et *e. g.* ostendere possemus, quemuis numerum primum formae $20n + 1$, vel $20n + 3$, vel $20n + 7$, vel $20n + 9$ (quippe quorum residuum -5) per alterutram formam $xx + 5yy$, $2xx + 2xy + 3yy$ repraesentari posse, et quidem numeros primos formae $20n + 1$ et $20n + 9$ per priorem, primos formae $20n + 3$, $20n + 7$, per posteriorem, nec non dupla primorum formae $20n + 1$, $20n + 9$ per formam $2xx + 2xy + 3yy$, dupla primorum formae $20n + 3$, $20n + 7$, per formam $xx + 5yy$: sed hanc propositionem infinitasque alias particulares quiuis proprio marte ex praecedentibus et infra tradendis deriuare poterit. — Transimus itaque ad *formas determinantis positiui*, et quum harum indoles prorsus alia sit, quando determinans est quadratus, alia, quando non-quadratus: formas determinantis quadrati hic primo excludimus posteaque seorsim considerabimus.

183. Problema. *Proposita forma quacunque (a, b, a'), cuius determinans positiuus non-quadratus $= D$: inuenire formam huic proprie aequiualentem, $(A,$*