ipsorum $x$, $y$ inter se primi sunt, praebebunt omnes repraesentationes ipsius $M$ in quibus diu. comm. max. valorum ipsorum $x$, $y$ est $\vartheta$ etc.

Palam igitur est, per praecepta praecedentia omnes repraesentationes numeri dati per formam datam determinantis negatiui inueniri posse.

182. Descendimus ad quosdam casus particulares, tum propter insignem ipsorum elegantiam, tum propter assiduam operam ab ill. Eulero ipsis impensam, vnde classicam quasi dignitatem sunt nacti.

I. Per formam $xx + yy$ ita repraesentari vt $x$ ad $y$ sit primus, (siue in duo quadrata inter se prima discerpi), nullus numerus potest nisi cuius residuum quadraticum est $= -1$, tales vero numeri, positiue accepti, omnes poterunt. Sit $M$ talis numerus, omnesque valores expr. $\sqrt{} -1 \pmod{M}$ hi: $N$, $-N$, $N'$, $-N'$, $N''$, $-N''$ etc. Tum per art. 176 forma $(M, N, \frac{NN+1}{M})$ formae $(1, 0, 1)$ proprie aequiualens erit. Sit transformatio aliqua propria huius in illam, $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, eruntque repraesentationes numeri $M$ per formam $xx + yy$ ad $N$ pertinentes hi quatuor *): $x = \pm \alpha$, $y = \pm \gamma$; $x = \mp \gamma$, $y = \pm \alpha$.

*) Patet enim, hunc casum sub (2) art. 180 contentum esse.

Quum forma (1, 0, 1) sit anceps, patet, etiam formam ($M$, — $N$, $\frac{NN \mp 1}{M}$) ipsi proprie aequiualentem fore, illamque proprie in hanc transmutari positis $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. Hinc deriuantur quatuor repraesentationes ipsius $M$ ad — $N$ pertinentes, $x = \pm \alpha$, $y = \mp \gamma$; $x = \pm \gamma$, $y = \mp \alpha$. Manifestum itaque est, octo repraesentationes ipsius $M$ dari, quarum semissis altera ad $N$, altera ad — $N$ pertineat; sed hae omnes *vnicam* tantummodo discerptionem numeri $M$ in duo quadrata exhibent, $M = \alpha\alpha + \gamma\gamma$, siquidem ad quadrata ipsa tantum, neque vero ad ordinem radicumue signa spectamus.

Quodsi itaque alii valores expr. $\sqrt{} - 1$ (mod. $M$) praeter $N$ et — $N$ non dantur, quod *e. g.* euenit, quando $M$ est numerus primus, $M$ vnico tantum modo in duo quadrata inter se prima resolui poterit. Iam quum — 1 sit residuum quadraticum cuiusuis numeri primi formae $4n + 1$ (art. 108), manifestoque numerus primus in duo quadrata inter se non prima discerpi nequeat, habemus theorema:

*Quiuis numerus primus formae* $4n + 1$ *in duo quadrata decomponi potest, et quidem vnico tantum modo.* $1 = 0 + 1$, $5 = 1 + 4$, $13 = 4 + 9$, $17 = 1 + 16$, $29 = 4 + 25$, $37 = 1 + 36$, $41 = 16 + 25$, $53 = 4 + 49$, $61 = 25 + 36$, $73 = 9 + 64$, $89 = 25 + 64$, $97 = 16 + 81$ etc.

Theorema hoc elegantissimum iam Fermatio notum fuit, sed ab ill. Eulero primo demonstratum est, *Comm. nou. Petr. T. V, ad annos* 1754, 1755, *p.* 3 *sqq.* In *T. IV*, diss. exstat ad idem argumentum pertinens, p 3 sqq., sed tum rem penitus nondum absoluerat, vid. imprimis art. 27.

Si igitur numerus aliquis formae $4n + 1$ aut pluribus modis aut nullo modo in duo quadrata resolui potest, certo non erit primus.

Vice versa autem, si expr. $\sqrt{\ } - 1$ (mod. $M$) praeter $N$ et $-N$ alios adhuc valores habet, aliae adhuc repraesentationes ipsius $M$ dabuntur, ad hos pertinentes. In hoc itaque casu $M$ pluribus modis in duo quadrata resolui poterit e. g. $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Repraesentationes reliquae, in quibus $x$, $y$ valores obtinent non primos inter se, per methodum nostram generalem facile inueniri possunt. Obseruamus tantummodo, si numerus aliquis factores formae $4n + 3$ inuoluens, per nullam diuisionem per quadratum ab his liberari possit (quod fiet, si aliquis aut plures talium factorum *dimensionem imparem* habet), hunc nullo modo in duo quadrata resolui posse *).

*) Si numerus $M = 2^{\mu} Sa^{\alpha} b^{\beta} c^{\gamma} \ldots$ ita vt $a$, $b$, $c$ etc. sint numeri primi inaequales formae $4n + 1$, atque $S$ productum ex omnibus factoribus primis ipsius $M$ formae $4n + 3$ (ad quam formam