$\pm pR(T+1)$, *non potest esse* $+(T+1)Np$, *siue* $-(T+1)Rp$. Hic casus supra fuit quintus.

Sit vt supra $e^2 = p + fa$ atque e par et $< a$.

I. Quando e per p non est diuisibilis, erit etiam f per p non diuisibilis. Praeterea autem erit f positiuus, formae $4n+1$ (siue A), atque $< a$; $+pRf$, adeoque (prop. 10 art. 132) $+fRp$. Sed est etiam $+faRp$, quare fiet $+aRp$, siue $-aNp$.

II. Quando e per p est diuisibilis, sit $e = pg$, atque $f = ph$. Erit itaque $g^2p = 1 + ha$. Tum h erit positiuus, formae $4n+3$ (B), et ad p et g^2 primus. Porro $+g^2pRh$, adeoque $+pRh$; hinc fit (prop, 13 art 132) $-hRp$. At est $-haRp$, vnde fit $+aRp$ atque $-aNp$.

139. *Casus tertius. Quando* $T+1$ *est formae* $4n+1$, $(=a)$, p *eiusdem formae, atque* $\pm pNa$: *non potest esse* $\pm aNp$. (Supra casus secundus).

Capiatur aliquis numerus primus ipso a minor, cuius non-residuum sit $+a$, quales dari supra demonstrauimus (art. 125, 129). Sed hic duos casus seorsim considerare oportet, prout hic numerus primus fuerit formae $4n+1$ vel $4n+3$; non enim demonstratum fuit, dari tales numeros primos *vtriusque* formae.

I. Sit iste numerus primus formae $4n+1$ et $= a'$. Tum erit $\pm a'Na$ (art. 137) adeoque

$\pm a'pRa$. Sit igitur $e^2 \equiv a'p$ (mod. a) atque e par, $< a$. Tunc iterum quatuor casus erunt distinguendi.

1) Quando e neque per p neque per a' est diuisibilis. Ponatur $e^2 = a'p \pm af$, signis ita acceptis vt f fiat positiuus. Tum erit $f < a$, ad a' et p primus atque pro signo superiori formae $4n + 3$, pro inferiori formae $4n + 1$. Designemus breuitatis gratia per $[x, y]$ multitudinem factorum primorum numeri y quorum non-residuum est x. Tum erit $a'pRf$ adeoque $[a'p, f] = 0$. Hinc erit $[f, a'p]$ numerus par, (prop. 1, 3, art. 133.), i. e. aut $= 0$ aut $= 2$. Quare erit f aut residuum vtriusque numerorum a', p, aut neutrius. Illud autem est impossibile, quum $\pm af$ sit residuum ipsius a', atque $\pm aNa'$ (hyp.); vnde fit $\pm fNa'$. Hinc f debet esse vtriusque numerorum a', p non-residuum. At propter $\pm af\,Rp$ erit $\pm aNp$. *Q. E. D.*

2) Quando e per p, neque vero per a' est diuisibilis, sit $e = gp$, atque $g^2p = a' \pm ah$, signo ita determinato, vt h fiat positiuus. Tum erit $h < a$, ad a', g, et p primus, atque pro signo superiori formae $4n + 3$, pro inferiori vero formae $4n + 1$. Ex aequatione $g^2p = a' \pm ah$ si per p, et a' multiplicatur, nullo negotio deduci potest, $pa'Rh \ldots\ldots (\alpha)$; $\pm ahpRa' \ldots (\beta)$ $aa'hRp \ldots\ldots (\gamma)$. Ex ($\alpha$) sequitur $[pa', h] = 0$, adeoque (prop, 1, 3, art. 153) $[h, pa']$ par, i. e. erit h non-residuum vel vtriusque p, a', vel

neutrius. *Priori in casu* ex (β) sequitur, $\pm apNa'$, et quum per hyp. sit $\pm aNa'$, erit $\pm pRa'$, Hinc per theor. fundam. quod pro numeris p', a' ipso $T + 1$ minoribus valet, $\pm a'Rp$. Hinc et ex eo quod hNp, fit per (γ) $\pm aNp$ *Q. E. D.* *Posteriori casu* ex (β) sequitur $\pm apRa'$, hinc $\pm pNa'$, $\pm a'Np$ hincque tandem et ex hRp fit ex (γ) $\pm aNp$ *Q. E. D.*

3) Quando e per a' non autem per p est diuisibilis. Pro hoc casu demonstratio tantum non eodem modo procedit vt in praec., neminemque qui hanc penetrauit poterit morari.

4) Quando e tum per a' tum per p est diuisibilis adeoque etiam per productum $a'p$ (numeros a',p enim *inaequales* esse supponimus, quia alias id quod demonstrare operam damus, esse aNa' iam in hypothesi aNp contentum foret), sit $e = ga'p$ atque $g^2a'p = 1 \pm ah$. Tum erit $h < a$, ad a' et p primus atque pro signo superiori formae $4n + 3$, pro inferiori formae $4n + 1$. Facile vero perspicitur, ex ista aequatione deduci posse haec $a'pRh$, $\pm ahpRa'$, $\pm aa'hRp$; quae cum iis quae in (2) inuenimus conueniunt. In reliquis autem demonstratio est eadem.

II. Quando iste numerus primus est formae $4n + 3$, demonstratio praecedenti tam similis est, vt eam apponere superfluum nobis visum sit. In eorum gratiam qui per se eam euoluere gestiunt (quod maxime commenda-