$m = 8$ vel altior potestas numeri 2, erit 1, 8; 3, 8; 5, 8; 7, 8 char. part. formae (a, b, c) pront $M \equiv 1; 3; 5; 7 \pmod{8}$ resp.

III. Vice versa si m est numerus primus aut numeri primi imparis potestas $= p^\mu$, determinantem $bb - ac$ metiens, atque M vel residuum vel non-residuum ipsius p, prout character formae (a, b, c) respectu ipsius p est Rp vel Np resp: erit $M(a, b, c)$ resid. quadr. ipsius m. Quando enim a per p non est diuisibilis, aM erit res. ipsius p adeoque etiam ipsius m; si itaque g est valor expr. $\surd\, aM \pmod{m}$, h valor expr. $\frac{bg}{a} \pmod{m}$, erit $gg \equiv aM$; $ah \equiv bg$ adeoque $agh \equiv bgg \equiv abM$ et $gh \equiv bM$; denique $ahh \equiv bgh \equiv bbM \equiv bbM - (bb - ac)M \equiv acM$ adeoque $hh \equiv cM$, i. e. (g, h) valor expr. $\surd\, M(a, b, c)$. Quando vero a per m est diuisibilis, certo c non erit; vnde facile perspicitur, eadem resultare, si pro h assumatur valor expr. $\surd\, cM \pmod{m}$, pro g valor expr. $\frac{bh}{c} \pmod{m}$.

Simili modo demonstratur, si m fuerit $= 4$ ipsumque $bb - ac$ metiatur, numerusque M accipiatur vel $\equiv 1$ vel $\equiv 3$ prout 1, 4 vel 3, 4 fuerit char. part. formae (a, b, c): fore $M(a, b, c)$ res. qu. ipsius m. Nec non, si m fuerit $= 8$ vel altior potestas ipsius 2 per quam $bb - ac$ diuisibilis sit, atque M accipiatur $\equiv 1; 3; 5; 7 \pmod{8}$ prout character part. formae (a, b, c) respectu numeri 8 postulet: $M(a, b, c)$ fore res. qu. ipsius m.

IV. Si determinans formae (a, b, c) est $= D$, atque $M(a, b, c)$ res. qu. ipsius D, omnes character particulares formae (a, b, c) tum respectu singulorum diuisorum primorum imparium ipsius D, tum respectu numeri 4 vel numeri 8 (si ipsum D metiuntur) ex numero M statim cognosci possunt. Ita e. g. quum $3(20, 10, 27)$ sit resid. qu. ipsius 440, scilicet $(150, 9)$ valor expr. $\sqrt{3(20, 10, 27)}$ sec. mod. 440, atque $3N5$, $3R11$: characteres formae $(20, 10, 27)$ sunt 3, 8; $N5$; $R11$. Soli characteres particulares respectu numerorum 4 et 8, quoties determinantem non metiuntur, nexum necessarium cum numero M non habent.

V. Vice versa, si numerus M ad D primus omnes characteres particulares formae (a, b, c) in se complectitur (exceptis characteribus respectu numerorum 4, 8, quando ipsum D non metiuntur): erit $M(a, b, c)$ res. qu. ipsius D. Nam ex III patet, si D sub formam $\pm A^\alpha B^\beta C^\gamma \ldots$ redigatur, ita vt A, B, C etc. sint numeri primi diuersi, fore $M(a, b, c)$ resid. qu. singulorum A^α, B^β, C^γ etc. Si igitur valor expr. $\sqrt{M(a, b, c)}$ secundum mod. A^α, est $(\mathfrak{A}, \mathfrak{A}')$; secundum mod. B^β, $(\mathfrak{B}, \mathfrak{B}')$; sec. mod. C^γ, $(\mathfrak{C}, \mathfrak{C}')$ etc. numerique g, h ita determinantur vt sit $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ etc.; $h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ etc. secundum modulos A^α, B^β, C^γ etc. resp. (art. 32): facile perspicietur, fore $gg \equiv aM$, $gh \equiv bM$, $hh \equiv cM$ secundum omnes modulos A^α, B^β, C^γ etc. adeoque etiam secundum modulum D qui illorum est productum.

VI. Propter has rationes numeri tales vt M vocabuntur *numeri characteristici* formae (a, b, c), poteruntque per V. plures huiusmodi numeri nullo negotio inueniri simulac omnes characteres particulares huius formae sunt eruti; simplicissimi autem tentando plerumque euoluuntur facillime. Manifestum est, si M sit numerus characteristicus formae primitiuae datae determinantis D, omnes numeros, ipsi M secundum mod. D congruos, fore numeros characteristicos eiusdem formae; formas in eadem classe, siue etiam in classibus diuersis ex eodem genere, contentas eosdem numeros characteristicos habere, quamobrem quiuis numerus characteristicus formae datae etiam toti classi et generi tribui potest; denique 1 semper esse numerum characteristicum formae classis et generis principalis, siue quamlibet formam e genere principali esse residuum determinantis sui.

VII. Si (g, h) est valor expr. $\sqrt{M(a, b, c)}$ (mod. m), atque $g' \equiv g$, $h' \equiv h$ (mod. m): erit etiam (g', h') valor eiusdem expressionis. Tales valores pro *aequiualentibus* haberi possunt; contra si (g, h), (g', h') sunt valores eiusdem expr. $\sqrt{M(a, b, c)}$, neque tamen simul $g' \equiv g$, $h' \equiv h$ (mod. m), *diuersi* sunt censendi. Manifesto quoties (g, h) est valor talis expressionis, etiam $(-g, -h)$ erit, facileque demonstratur, hos valores semper esse diuersos nisi $m = 2$. Aeque facile demonstratur, expressionem $\sqrt{M(a, b, c)}$ (mod. m) plures valores diuersos quam duos tales (oppositos) habere non posse, quando m sit aut numerus primus impar aut nu-