cundum productum ex his congrui erunt. Quum enim $m - n$ per singulos a, b, c etc. sit diuisibilis, etiam per eorum productum diuidi poterit.

Denique *si a ad b primus et ak per b diuisibilis, erit etiam k per b diuisibilis.* Namque quoniam ak tam per a quam per b diuisibilis, etiam per ab diuidi poterit, i. e $\frac{ak}{ab} = \frac{k}{b}$ erit integer.

20. *Quando $A = a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, est potestas aliqua, puta $= k^n$: omnes exponentes α, β, γ etc. per n erunt diuisibiles.*

Numerus enim k alios factores primos quam a, b, c etc. non inuoluit. Contineat factorem a, α^1 vicibus, continebitque k^n siue A hunc factorem $n\alpha^1$ vicibus; quare $n\alpha^1 = \alpha$, et $\frac{\alpha}{n}$ integer. Similiter $\frac{\beta}{n}$ etc. integros esse demonstratur.

21. *Quando a, b, c etc. sunt inter se primi, et productum abc etc. potestas aliqua, puta $= k^n$: singuli numeri a, b, c etc. similes potestates erunt.*

Sit $a = l^\lambda m^\mu p^\pi$ etc., designantibus l, m, p etc. numeros primos diuersos, quorum nullus per *hyp.* est factor numerorum b, c etc. Quare productum abc etc. factorem l implicabit λ vicibus, factorem m vero μ vicibus etc.: hinc (*art. praec.*) λ, μ, π etc. per n diuisibiles adeoque $\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}}$ etc. integer. Similiter de reliquis b, c etc.

Haec de numeris primis praemittenda erant; iam ad ea quae finem nobis propositum propius attinent conuertimur.

22. *Si numeri a, b per alium k diuisibiles secundum modulum m ad k primum sunt congrui:* $\frac{a}{k}$ *et* $\frac{b}{k}$ *secundum eundem modulum congrui erunt.*

Patet enim $a - b$ per k diuisibilem fore, nec minus per m (*hyp.*); quare (*art.* 19) $\frac{a-b}{k}$ per m diuisibilis erit, i. e. erit $\frac{a}{k} \equiv \frac{b}{k}$ (mod. m.).

Si autem reliquis manentibus m et k habent diuisorem communem maximum e, erit $\frac{a}{k} \equiv \frac{b}{k}$ (mod. $\frac{m}{e}$). Namque $\frac{k}{e}$ et $\frac{m}{e}$ inter se primi. At $a - b$ tam per k quam per m diuisibilis adeoque etiam $\frac{a-b}{e}$ tam per $\frac{k}{e}$ quam per $\frac{m}{e}$, hincque per $\frac{km}{ee}$ i. e. $\frac{a-b}{k}$ per $\frac{m}{e}$, siue $\frac{a}{k} \equiv \frac{b}{k}$ (mod. $\frac{m}{e}$).

23. *Si a ad m primus, et e, f numeri secundum modulum m incongrui: erunt etiam ae, af incongrui secundum m.*

Hoc est tantum conuersio theor. art. praec.

Hinc vero manifestum est, si a per omnes numeros integros a 0 vsque ad $m - 1$ multiplicetur productaque secundum modulum m ad residua sua minima reducantur, haec omnia fore inaequalia. Et quum horum residuorum, quorum nullum $> m$, numerus sit m, totidemque dentur numeri a 0 usque ad $m - 1$, patet, nullum horum numerorum inter illa residua deesse posse.

24. *Expressio* $ax + b$, denotantibus a, b numeros datos, x numerum indeterminatum seu variabilem, *secundum modulum m, ad a primum, cuiuis numero dato congrua fieri potest.*

Sit numerus, cui congrua fieri debet, c, et residuum minimum positiuum ipsius $c - b$ secundum modulum m, e. Ex art. praec. necessario datur valor ipsius $x < m$, talis, vt producti ax secundum modulum m residuum minimum fiat e; esto hic valor v, eritque $av \equiv e \equiv c - b$; vnde $av + b \equiv c \pmod{m}$ *Q. E. F.*

25. Expressionem duas quantitates congruas exhibentem ad instar aequationum, *congruentiam* vocamus; quae si incognitam implicat, *resolui* dicitur, quando pro hac valor inuenitur congruentiae satisfaciens (*radix*). Hinc porro intelligitur, quid sit *congruentia resolubilis et congruentia irresolubilis*. Tandem facile perspicitur similes distinctiones locum hic habere posse vti in aequationibus. Congruentiarum *transscendentium* infra exempla occurrent; *algebraicae* vero secundum dimensionem maximam incognitae in congruentias primi, secundi altiorumque *graduum* distribuuntur. Nec minus congruentiae plures proponi possunt plures incognitas inuoluentes, de quarum *eliminatione* disquirendum.

26. Congruentia itaque primi gradus, $ax + b \equiv c$ ex art. 24 semper resolubilis, quando modulus ad a est primus. Quodsi vero v fuerit valor idoneus ipsius x, siue radix congruentiae, palam est, omnes numeros, ipsi v secundum congruentiae propositae modulum congruos, etiam radices fore (art. 9.) Neque minus facile perspicitur, omnes radices ipsi v congruos esse debere: si enim alia radix fuerit t, erit $av + b \equiv at + b$. vnde $av \equiv at$, et hinc $v \equiv t$ (art. 22). Hinc colligitur congruentiam $x + v$