Dem. Consideremus primo duos tantum numeros A, B, sitque horum diuisor maximus communis $= \lambda$. Tum congruentia $Ax \equiv \lambda$ (mod. B) erit resolubilis (art. 30). Sit radix $\equiv \alpha$, ponaturque $\frac{\lambda - A\alpha}{B} = \beta$. Tum erit $\alpha A + \beta B = \lambda$, vti desiderabatur.

Accedente numero tertio C, sit maximus diuisor communis numerorum λ, C, $= \lambda'$, eritque hic simul maximus diuisor communis numerorum A, B, C *). Determinentur numeri k, γ ita vt sit $k\lambda + \gamma C = \lambda'$, eritque $k\alpha A + k\beta B + \gamma C = \lambda'$.

Accedente numero quarto D, ponatur maximus diuisor communis numerorum λ', D (quem simul esse maximum diuisorem communem numerorum A, B, C, D facile perspicitur) $= \lambda''$, fiatque $k'\lambda' + \delta D = \lambda''$. Tum erit $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

Simili modo procedi potest, quotcunque alii numeri accedant.

Si itaque numeri A, B, C, D etc. diuisorem communem non habent, patet fieri posse $aA + bB + cC +$ etc. $= 1$.

41. *Si p est numerus primus atque habentur p res, inter quas quotcunque aequales esse possunt, modo non omnes sint aequales: numerus permutationum harum rerum per p erit diuisibilis.*

*) Metietur enim manifesto λ' omnes A, B, C. Si vero non esset diuisor communis *maximus*: maximus foret maior quam λ'. Iam quoniam hic diuisor maximus metitur ipsos A B; metietur etiam ipsum $\alpha A + \beta B$ i. e. ipsum λ, maior minorem *Q. E. A.* — Facilius adhuc hoc ex art. 18 deduci potest.

Exempl. Quinque res A, A, A, B, B, decem modis diuersis possunt transponi.

Demonstratio huius theorematis facile quidem ex nota permutationum theoria peti potest. Si enim inter has res sunt primo a aequales nempe $= A$, tum b aequales nempe $= B$, tum c aequales nempe $= C$ etc. (vbi numeri a, b, c etc. etiam unitatem designare possunt), ita vt habeatur $a + b + c +$ etc $= p$, numerus permutationum erit $= \frac{1 \cdot 2 \cdot 3 \ldots p}{1 \cdot 2 \cdot 3 \ldots a \cdot 1 \cdot 2 \ldots b \cdot 1 \cdot 2 \ldots c \text{ etc.}}$. Iam per se clarum est, huius fractionis numeratorem per denominatorem diuisibilem esse, quoniam numerus permutationum debet esse integer: at numerator per p diuisibilis est, denominator vero, qui ex factoribus ipso p minoribus est compositus, per p non diuisibilis (art. 15). Quare numerus permutationum per p erit diuisibilis (art. 19).

Speramus tamen fore quibus etiam sequens demonstratio haud ingrata sit futura.

Quando in duabus permutationibus rerum e quibus compositae sunt ordo in eo tantum discrepat, vt ea res quae in altera primum locum occupat, aliam sedem in altera teneat, reliquae autem eodem in vtraque ordine progrediuntur, eamque quae in altera vltima est, ea quae est prima, in altera excipit; *permutationes similes* vocemus *). Ita in ex. nostro permutationes $ABAAB$ et $ABABA$ similes erunt,

*) Si permutationes similes in circulum scriptae esse concipiuntur ita vt vltima res primae fiat contigua, nulla omnino erit discrepantia, quoniam nullus locus primus aut vltimus vocari poterit,

quoniam res quae in priori primum secundum etc. locum occupant, in posteriori loco tertio quarto etc. eodem ordine sunt collocatae.

Iam quoniam quaeque permutatio ex p rebus constat, patet cuiuis $p - 1$ similes adinueniri posse, si ea res quae prima fuerat, ad secundum, tertium etc. locum promoueatur. Quarum si nullae identicae esse possunt manifestum est, omnium permutationum numerum per p diuisibilem euadere, quippe qui p vicibus maior sit quam numerus omnium permutationum dissimilium. Supponamus igitur duas permutationes $PQ \ldots TV \ldots YZ$; $V \ldots YZPQ \ldots T$, quarum altera ex altera per terminorum promotionem orta sit, identicas esse siue $P = V$ etc. Sit terminus P qui in priori est primus, $n + 1$ *tus* in posteriori. Erit igitur in serie posteriori terminus $n + 1$ *tus* aequalis primo, $n + 2$ *tus* secundo etc. vnde $2n + 1$ *tus* rursus primo aequalis euadet, eademque ratione $3n + 1$ *tus* etc.; generaliterque terminus $kn + m$ *tus* m *to* (vbi quando $kn + m$ ipsum p superat, aut series $V \ldots YZPQ \ldots T$ semper ab initio repeti concipienda est, aut a $kn + m$ multiplum ipsius p proxime minus rescindendum). Quamobrem si k ita determinatur, vt fiat $kn \equiv 1 \pmod{p}$, quod fieri potest quia p primus, sequitur generaliter terminum m *tum* $m + 1$ *to* aequalem esse, siue quemuis terminum sequenti, i. e. omnes terminos aequales esse contra hypothesin.

42. *Si coefficientes* $A, B, C \ldots N$; $a, b, c \ldots n$ *duarum functionum formae*