

Per inductionem autem circa numeros sequentes institutam, inuenitur:

— 7, — 11, + 13, + 17, — 19, — 23, + 29, — 31, + 37, + 41, — 43, — 47, + 53, — 59 etc. esse residua vel non-residua omnium numerorum primorum, qui, positiui sumti, illorum primorum respectiue sint residua vel non-residua. Inductio haec perfacile adiumento tabulae II confici potest.

Quiuis autem leui attentione adhibita obseruabit, ex his numeris primis signo positiuo affectos esse eos, qui sint formae $4n + 1$, negatiuo autem eos, qui sint formae $4n + 3$.

131. Quod hic per inductionem deteximus, generaliter locum habere mox demonstrabimus. Antequam autem hoc negotium adeamus, necesse erit, omnia quae ex theoremate, si verum esse supponitur, sequuntur, eruere. Theorema ipsum ita enunciamus.

Si p est numerus primus formae $4n + 1$, erit $+ p$, si vero p formae $4n + 3$, erit $- p$ residuum vel non-residuum cuiusuis numeri primi qui positue acceptus ipsius p est residuum vel non-residuum.

Quia omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur, denominatio theoremat^{is} fundamentalis, qua in sequentibus vtemur, haud absona erit.

Vt ratiocinia nostra quam breuissime exhiberi possint, per a, a', a'' etc. numeros primos

formae $4n + 1$, per b, b', b'' etc. numeros primos formae $4n + 3$ denotabimus; per A, A', A'' etc. numeros quoscunque formae $4n + 1$, per B, B', B'' etc. autem numeros quoscunque formae $4n + 3$; tandem littera R duabus quantitatibus interposita indicabit, priorem sequentis esse residuum, sicuti littera N significationem contrariam habebit. Ex. gr. $+ 5R11, \pm 2N5$, indicabit $+ 5$ ipsius 11 esse residuum, $+ 2$ vel $- 2$ esse ipsius 5 non-residuum. Iam collato theoremate fundamentali cum theorematibus art. 111, sequentes propositiones facile deducuntur.

Si erit

- $$\begin{array}{ll}
1. & \pm a R a' \dots \dots \pm a' R a \\
2. & \pm a N a' \dots \dots \pm a' N a \\
3. & \left[\begin{array}{l} + a R b \\ - a N b \end{array} \right] \dots \dots \pm b R a \\
4. & \left[\begin{array}{l} + a N b \\ - a R b \end{array} \right] \dots \dots \pm b N a \\
5. & \pm b R a \dots \dots \left[\begin{array}{l} + a R b \\ - a N b \end{array} \right] \\
6. & \pm b N a \dots \dots \left[\begin{array}{l} + a N b \\ - a R b \end{array} \right] \\
7. & \left[\begin{array}{l} + b R b' \\ - b N b' \end{array} \right] \dots \dots \left[\begin{array}{l} + b' N b \\ - b' R b \end{array} \right] \\
8. & \left[\begin{array}{l} + b N b' \\ - b R b' \end{array} \right] \dots \dots \left[\begin{array}{l} + b' R b \\ - b' N a \end{array} \right]
\end{array}$$

132. In his omnes casus, qui, duos numeros primos comparando, occurrere possunt, continentur: quae sequuntur, ad numeros quoscunque pertinent: sed harum demonstrationes minus sunt obuiaae.

Si erit

$$9. \quad \pm a R A \dots, \pm A R a$$

$$10. \quad \pm b R A \dots \left\{ \begin{array}{l} + A R b \\ - A N b \end{array} \right.$$

$$11. \quad + a R B \dots, \pm B R a$$

$$12. \quad - a R B \dots, \pm B N a$$

$$13. \quad + b R B \dots \left\{ \begin{array}{l} - B R b \\ + B N b \end{array} \right.$$

$$14. \quad - b R B \dots \left\{ \begin{array}{l} - B R b \\ + B N b \end{array} \right.$$

Quum omnium harum propositionum demonstrationes ex iisdem principiis sint petendae, necesse non erit omnes euoluere: demonstratio prop. 9, quam apponimus tamquam exemplum inseruire potest. Ante omnia autem obseruetur, quemuis numerum formae $4n + 1$ aut nullum factorem formae $4n + 3$ habere, aut duos, aut quatuor etc. i. e. multitudinem talium factorum (inter quos etiam aequales esse possunt) semper fore parem: quemuis vero formae $4n + 3$ multitudinem imparem factorum formae $4n + 3$ (i. e. aut vnum aut tres aut