7 . . . . . 1, 2, 4.
11 . . . . . 1, 3, 4, 5, 9.
13 . . . . . 1, 3, 4, 9, 10, 12.
17 . . . . . 1, 2, 4, 8, 9, 13, 15, 16.
etc.

reliqui vero numeri, his modulis minores non residua.

98. Theorema. *Productum e duobus residuis quadraticis numeri primi p, est residuum; productum e residuo in non residuum, est non residuum; denique productum e duobus non-residuis, residuum.*

Demonstr. I. Sint A, B residua e quadratis aa, bb oriunda siue $A \equiv aa$, $B \equiv bb$, eritque productum AB quadrato numeri ab congruum i. e. residuum.

II. Quando A est residuum, puta $\equiv aa$, B vero non residuum, AB erit non-residuum. Ponatur enim si fieri potest $AB \equiv kk$, sitque valor expressionis $\frac{k}{a}$ (mod. p) $\equiv b$; erit itaque $aaB \equiv aabb$, vnde $B \equiv bb$, i. e. B residuum contra hyp.

Aliter. Multiplicentur omnes numeri qui inter hos 1, 2, 3. . . . $p - 1$ sunt residua (quorum multiudo $= \frac{1}{2}(p - 1)$, per A omniaque producta erunt residua quadratica, et quidem erunt omnia incongrua. Iam si non-residuum B per A multiplicatur, productum nulli productorum quae iam habentur congruum erit; quare si residuum esset, haberentur $\frac{1}{2}(p + 1)$ residua incongrua inter quae nondum est residuum 0, contra art. 96.

III. Sint A, B, non-residua. Multiplicentur omnes numeri qui inter hos 1, 2, 3.... $p-1$ sunt residua per A, habebunturque $\frac{1}{2}(p-1)$ non-residua inter se incongrua (II); iam productum AB nulli illorum congruum esse potest; quodsi igitur esset non-residuum, haberentur $\frac{1}{2}(p+1)$ non-residua inter se incongrua, contra art. 95. Quare productum etc. *Q. E. D.*

Facilius adhuc haec theoremata e principiis sect. praec. deriuantur. Quia enim residuorum indices semper sunt pares, non-residuorum vero impares, index producti e duobus residuis vel non-residuis erit par, adeoque productum ipsum, residuum. Contra index producti e residuo in non-residuum erit impar adeoque productum ipsum non-residuum.

Vtraque demonstrandi methodus etiam pro his theorematibus adhiberi potest: *Expressionis* $\frac{a}{b}$ *(mod. p) valor erit residuum, quando numeri a, b simul sunt residua, vel simul non residua; contra autem erit non-residuum, quando numerorum a, b alter est residuum alter non-residuum.* Possunt etiam ex conuersione theorr. art. praec. obtineri.

99. Generaliter, productum ex quotcunque factoribus est residuum tum quando omnes sunt residua, tum quando non residuorum, quae inter eos occurrunt, multitudo est par; quando vero multitudo non residuorum quae inter factores reperiuntur est impar, productum erit non-residuum. Facile itaque diiudicari potest,

vtrum numerus compositus sit residuum, necne, si modo quid sint singuli ipsius factores constet. Quamobrem in tabula II numeros primos tautummodo recepimus. Oeconomia huius tabulae haec est. In margine positi sunt moduli,*) in facie vero numeri primi successiui; quando ex his aliquis fuit residuum moduli alicuius, in spatio vtrique respondente lineola collocata est, quando vero numerus primus fuit non residuum moduli, spatium respondens vacuum mansit.

100. Antequam ad difficiliora progrediamur, quaedam de modulis non primis adiicienda sunt.

Si numeri primi p, potestas aliqua p^n pro modulo assumitur (vbi p non esse 2 supponimus), omnium numerorum per p non diuisibilium moduloque minorum altera semissis erunt residua, altera non residua, i. e. vtrorumque multitudo $= \frac{1}{2}(p-1)p^{n-1}$.

Si enim r est residuum: quadrato alicui congruus erit, cuius radix moduli dimidium non superat, vid. art. 94. Iam facile perspicitur, dari $\frac{1}{2}(p-1)p^{n-1}$ numeros per p non diuisibiles modulique semisse minoribus; superest itaque vt demonstretur, omnium horum numerorum quadrata incongrua esse, siue residua quadratica diuersa suppeditare. Quodsi duorum numerorum a, b per p non diuisibilium

*) Quomodo etiam modulis compositis carere possimus mox docebimus,