ipsius q non-residuum erit (art. 112), adeoque etiam $2a^2$ *) et $8n + 5$. *Q. E. D.*

126. Sed numerum quemuis primum formae $8n + 1$ positiue acceptum semper alicuius numeri primi ipso minoris non residuum esse, per artificia tam obuia demonstrari nequit. Quum autem haec veritas maximi sit momenti, demonstrationem rigorosam, quamuis aliquantum prolixa sit, praeterire non possumus. Praetermittus sequens

LEMMA. *Si habentur duae series numerorum, A, B, C, etc. . . . . (I), A', B', C', etc. . . . . (II),* (vtrum terminorum multitudo in vtraque idem sit necne nihil interest) *ita comparatae, vt, denotante p numerum quemcunque primum aut numeri primi potestatem, terminum aliquem secundae seriei (siue etiam plures) metientem, totidem ad minimum termini in serie prima sint per p diuisibiles, quot sunt in secunda: tum dico productum ex omnibus numeris (I) diuisibile fore per productum ex omnibus numeris (II).*

Exempl. Constet (I) e numeris 12, 18, 45; (II) ex his 3, 4, 5, 6, 9. Tum diuisibiles erunt per 2, 4, 3, 9, 5 in (I) 2, 1, 3, 2, 1 termini, in (II) 2, 1, 3, 1, 1 termini, respectiue; productum autem omnium terminorum (I) = 9720 diuisibile est per productum omnium terminorum (II), 3240.

*) Art 98. Patet enim a^2 esse residuum ipsius q per q non diuisibile, nam alias etiam numerus primus p per q foret diuisibilis. *Q. E. A.*

Demonstr. Sit productum ex omnibus terminis (I) $= Q$, productum omnium terminorum seriei (II), $= Q'$. Patet quemuis numerum primum qui sit diuisor ipsius Q' etiam ipsius Qdiuisorem fore. Iam ostendemus quemuis factorem primum ipsius Q', in Q totidem ad minimum dimensiones habere quot habeat in Q'. Esto talis diuisor p, ponaturque, in serie (I) a terminos esse per p diuisibiles neque vero per p^2, b terminos per p^2 non autem per p^3 diuisibiles, c terminos per p^3 non autem per p^4 etc. similia denotent literae a', b', c' etc. pro serie (II), perspicieturque facile, p in Q habere $a + b + c +$ etc. dimensiones, in Q' vero $a' + b' + c' +$ etc. At a' certe non maior quam a, b' non maior quam b etc. (hyp.); quare $a' + b' + c'$ etc. certo non erit $> a + b + c$ etc. — Quum itaque nullus numerus primus in Q' plures dimensiones habere possit, quam in Q, Q per Q' diuisibilis erit (art. 17) *Q. E. D.*

127. Lemma. *In progressione* 1, 2, 3, 4.... n, *plures termini esse nequeunt per numerum quemcunque* h *diuisibiles, quam in hac* $a, a + 1, a + 2, \ldots\ldots a + n - 1$ *ex totidem terminis constante.*

Nullo enim negotio perspicitur si n fuerit multiplum ipsius h, in vtraque progressione $\frac{n}{h}$ terminos fore per h diuisibiles; sin minus, ponatur $n = h + f$, ita vt f sit $< h$, eruntque in priori serie e termini per h diuisibiles, in posteriori autem vel totidem vel $e + 1$.

Hinc tamquam Coroll. sequitur propositio ex numerorum figuratorum theoria nota, sed a nemine, ni fallimur, hactenus directe demonstrata, $\frac{a \cdot a+1 \cdot a+2 \ldots a+n-1}{1 \cdot 2 \cdot 3 \ldots n}$ semper esse numerum integrum.

Denique Lemma hoc generalius ita proponi potuisset:

In progressione a, $a+1$, $a+1$, ... $a+n-1$ totidem ad minimum dantur termini secundum modulum h numero cuicunque dato, r, congrui, quot in hac, 1, 2, 3.... n termini per h diuisibiles.

128. Theorema. *Sit a numerus quicunque formae $8n+1$, p numerus quicunque ad a primus, cuius residuum $+a$, tandem m numerus arbitrarius: tum dico, in progressione a, $\frac{1}{2}(a-1)$, $2(a-4)$, $\frac{1}{2}(a-9)$, $2(a-16)$, ... $2(a-m^2)$, vel $\frac{1}{2}(a-m^2)$, prout m par vel impar, totidem ad minimum dari terminos per p diuisibiles quot dentur in hac 1, 2, 3.... $2m+1$.* Priorem progressionem designamus per (I) posteriorem per (II).

Demonstr. I. Quando $p = 2$, in (I) omnes termini praeter primum, i. e. m termini diuisibiles erunt; totidem autem erunt in (II).

II. Sit p numerus impar, vel numeri imparis duplum vel quadruplum, atque $a \equiv rr \pmod{p}$. Tum in progressione, $-m$, $-(m-1)$, $-(m-2)$ ..... $+m$ (quae terminorum multitudine cum (I) et (II) conuenit et per