nobis reseruamus, quando forsan fusius quantitatum imaginarium theoriam, quae nostro quidem iudicio a nemine hactenus ad notiones claras est reducta, pertractare suscipiemus. Periti hunc algorithmum facile ipsi eruent: qui minus sunt excercitati, perinde tamen tabula hac vti poterunt, vt ii qui recentiorum commenta de *logarithmis* imaginariis ignorant, logarithmis vtuntur, si quidem principia supra stabilita probe tenuerint.

92. Secundum modulum e pluribus primis compositum tantum non omnia quae ad residua potestatum pertinent ex theoria congruentiarum generali deduci possunt; quia vero infra congruentias quascunque secundum modulum e pluribus primis compositum ad congruentias, quarum modulus est primus aut primi potestas, reducere fusius docebimus, non est quod huic rei multum hic immoremur. Obseruamus tantum, bellissimam proprietatem, quae pro reliquis modulis locum habeat, quod scilicet semper exstent numeri quorum periodus omnes numeros ad modulum primos complectatur, hic deficere, excepto vnico casu, quando scilicet modulus est duplum numeri primi, aut potestatis numeri primi. Si enim modulus m redigitur ad formam $A^{a}B^{b}C^{c}$ etc. designantibus A, B, C etc. numeros primos diuersos, praeterea A^{a-1} $(A-1)$ disignatur per α, B^{b-1} $(B-1)$ per β etc. denique z est numerus ad m primus; erit $z^{\alpha} \equiv 1 \pmod{A^{a}}$ $z^{\beta} \equiv 1 \pmod{A^{b}}$ etc. Quodsi igitur μ est minimus numerorum α, β, γ etc. diuiduus communis, erit

$x^\mu \equiv 1$ secundum omnes modulos A^a, B^b etc. adeoque etiam secundum m, cui illorum productum est aequale. At excepto casu vbi m est duplum numeri primi aut potestatis numeri primi, numerorum α, β, γ etc. diuiduus communis minimus, ipsorum producto est minor (quoniam numeri α, β, γ etc. inter se primi esse nequeunt sed certe diuisorem 2 communem habent). Nullius itaque numeri periodus tot terminos comprehendere potest, quot dantur numeri ad modulum primi ipsoque minores, quia horum numerus producto ex α, β, γ etc. est aequalis. Ita ex. gr. pro $m = 1001$ cuiusuis numeri ad m primi potestas exponentis 60 vnitati est congrua, quia 60 est diuiduus communis numerorum 6, 10, 12. — Casus autem vbi modulus est duplum numeri primi aut duplum potestatis numeri primi illi vbi est primus aut primi potestas prorsus est similis.

93, Scriptorum in quibus alii geometrae de argumento in hac sectione pertractato egerunt, iam passim mentio est facta. Eos tamen qui quaedam fusius, quam nobis breuitas permisit, explicata desiderant, ablegamus imprimis ad sequentes ill. Euleri commentationes, ob perspicuitatem qua vir summus prae omnibus semper excelluit, maxime commendabiles.

Theoremata circa residua ex diuisione potestatum relicta. Com. nou. Petr. T. VII. p. 49. sqq.

Demonstrationes circa residua ex diuisione potestatum per numeros primos resultantia. Ibid. T. XVIII. p. 85 sqq.

Adiungi his possunt *Opusculorum analyt.* T. I, *dissertt.* 5 et 8.

Sectio Qvarta

de

CONGRVENTIIS SECVNDI GRADVS.

94. Theorema. *Numero quocunque, m, pro modulo accepto, ex numeris 0, 1, 2, 3.... $m-1$, plures quam $\frac{1}{2}m+1$ quando m est' par, siue plures quam $\frac{1}{2}m+\frac{1}{2}$, quando m est impar quadrato congrui fieri non possunt.*

Dem. Quoniam numerorum congruorum quadrata sunt congrua: quiuis numerus, qui vlli quadrato congruus fieri potest, etiam quadrato alicui cuius radix $< m$ congruus erit. Sufficit itaque residua minima quadratorum 0, 1, 4, 9.... $(m-1)^2$ considerare. At facile perspicitur, esse $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$ etc. Hinc etiam, quando m est par, quadratorum $\frac{1}{2}(m-1)^2$ et $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ et $(\frac{1}{2}m+2)^2$ etc. residua minima eadem erunt: quando vero m est impar, quadrata $(\frac{1}{2}m-\frac{1}{2})^2$ et $(\frac{1}{2}m+\frac{1}{2})^2$; $(\frac{1}{2}m-\frac{3}{2})^2$ et $(\frac{1}{2}m+\frac{3}{2})^2$ etc. erunt congrua. Vnde palam est, alios numeros, quam qui alicui ex quadratis 0, 1,