# LETTRE XXXIX.

=

EULER à GOLDBACH.

SOMMAIRE. Théorèmes de la théorie des nombres

---

Berlin d. 6 März 1742.

— — Dass $4mn - m - 1$ oder $4mn - m - n$ niemals ein quadratum seyn könne, konnte ich bis anjetzo auch nicht rigorose demonstriren, sondern ich hatte solches aus einem theoremate Fermatiano, worin behauptet wird, dass eine summa duorum quadratorum $aa + bb$ niemals per numerum formae $4n - 1$ divisibilis sey, hergeleitet. Denn hat dieses theorema seine Richtigkeit, so ist $aa + 1 \equiv (4n - 1)m$, da ich Ew. signum $\equiv$ um eine aequationem impossibilem anzuzeigen, gebrauche. Dahero ist $aa \equiv 4mn - m - 1$. Ferner kann auch $\frac{aa+1}{4n-1}$ unmöglich ein numerus integer seyn, oder es ist $\frac{aa+1}{4n-1} \equiv i$, folglich ist auch $\frac{aa+1}{4n-1} + 1$ oder



$\frac{aa+4n}{4n-1}$ oder $\frac{bb+n}{4n-1} \equiv i$. Gleichfalls kann $\frac{bb+n}{4n-1} + n$ oder $\frac{bb+4nn}{4n-1}$ oder $\frac{cc+nn}{4n-1}$ kein numerus integer seyn. Und wenn man auf solche Art fortgehet, so folget, dass $\frac{aa+n^a}{4n-1} \equiv m$ und also $aa \equiv 4mn - m - n^a$; welches die Consequenz ist, so Ew. aus diesem theoremate gezogen haben. Die Richtigkeit davon beruhet also auf der Wahrheit dieses theorematis, dass eine summa duorum quadratorum $aa + bb$ unmöglich durch $4n - 1$ getheilt werden könne, wenn nicht $aa$ und $bb$ ein jedes für sich durch $4n - 1$ divisibile ist. Ich habe aber erst jetzo hievon nachfolgende Demonstration gefunden:

*Prop.* 1. Haec forma $(a + b)^p - a^p - b^p$ semper est divisibilis per $p$ si fuerit $p$ numerus primus.

*Dem.* Evolvatur potestas $(a + b)^p$ eritque

$$(a+b)^p - a^p - b^p = \frac{p}{1}a^{p-1}b + \frac{p(p-1)}{1.2}a^{p-2}b^2 + \ldots\ldots + \frac{p(p-1)}{1.2}a^2b^{p-2} + \frac{p}{1}ab^{p-1}$$

cujus expressionis singuli termini sunt numeri integri, singuli ergo erunt divisibiles per $p$ siquidem $p$ sit numerus primus: nam si $p$ foret numerus compositus, fieri possit, ut in quodam termino factor quispiam ipsius $p$ per factorem denominatoris tolleretur, illeque terminus, ac proinde tota expressio cessaret per $p$ divisibilis esse. Quocirca si $p$ est numerus primus, haec expressio $(a + b)^p - a^p - b^p$ semper erit divisibilis per $p$. *Q.E.D.*

*Coroll.* 1. Positis ergo $a = b = 1$ erit $2^p - 2$ divisibile per numerum primum $p$, ideoque nisi $p$ sit $= 2$ erit $2^{p-1} - 1$ per $p$ divisibile.

*Coroll.* 2. Sit $a = 2$, $b = 1$, erit $3^p - 2^p - 1$ divisibile per $p$. Cum autem $2^p - 2$ sit quoque divisibile per $p$, erit quoque istarum formularum summa $3^p - 3$ divisibilis per $p$, ideoque nisi sit $p = 3$, erit $3^{p-1} - 1$ per $p$ divisibile.

*Prop.* 2. Si $a^p - a$ fuerit divisibile per $p$ erit quoque $(a+1)^p - a - 1$ per $p$ divisibile.

*Dem.* Si in propositione 1 ponatur $b = 1$, erit $(a+1)^p - a^p - 1$ per $p$ divisibile. Cum autem per hypothesin sit $a^p - a$ per $p$ divisibile, erit quoque summa istarum formularum $(a+1)^p - a - 1$ per $p$ divisibilis $Q.E.D.$

*Coroll.* 1. Cum igitur $1^p - 1$ divisibile sit per $p$, erit quoque $2^p - 2$ divisibile per $p$, hincque porro progrediendo per $p$ divisibiles erunt istae formulae $3^p - 3$, $4^p - 4$, $5^p - 5$, etc.

*Coroll.* 2. Generaliter ergo per numerum primum $p$ divisibilis erit ista formula $a^p - a$ quicunque numerus integer loco $a$ ponatur. Nisi ergo $p$ sit divisor ipsius $a$, erit quoque $a^{p-1} - 1$ per $p$ divisibile.

*Coroll.* 3. Quoniam simili modo $b^{p-1} - 1$ per numerum primum $p$ est divisibile, nisi $b$ sit multiplum ipsius $p$, sequitur fore $a^{p-1} - b^{p-1}$ per $p$ divisibile.

*Theorema.* Summa duorum quadratorum $aa + bb$ non est divisibilis per numerum primum $4n-1$, nisi utrumque quadratum seorsim per eundem numerum primum sit divisibile.

*Demonstratio.* Quoniam per hyp. neque $a$ neque $b$ divisibile est per $4n-1$, sequitur hanc formulam $a^{4n-2} - b^{4n-2}$ fore per $4n-1$ divisibilem, unde per $4n-1$ non erit divisibilis haec forma $a^{4n-2} + b^{4n-2}$ neque propterea ullus ejus factor. At cum $4n-2$ sit numerus impariter par, formulae $a^{4n-2} + b^{4n-2}$ factor est $aa + bb$: quocirca $aa + bb$ per numerum primum $4n-1$ dividi omnino nequit. $Q.E.D.$



*Coroll.* 1. Quoniam si $4n-1$ non est numerus primus, divisorem habet necessario numerum primum hujus formae $4n-1$, sequitur summam duorum quadratorum $aa + bb$ per nullum numerum hujus formae $4n-1$ sive primum, sive non primum dividi posse.

*Coroll.* 2. Quodsi ergo summa duorum quadratorum $aa+bb$ habeat divisorem, is erit necessario numerus formae hujus $4n+1$.

*Coroll.* 3. Si ergo summa duorum quadratorum $aa+bb$ per alium numerum dividi nequit, nisi qui ipse sit duorum quadratorum summa (quod demonstrari posse confido) sequitur omnem numerum primum $4n+1$ in duo quadrata esse resolubilem.

Dass Ew. die curiosité gehabt zu untersuchen, wann diese Formul $2^{+p\sqrt{-1}} + 2^{-p\sqrt{-1}}$ nihilo aequalis werden könnte, hat mir Anlass gegeben anzumerken, dass solches infinitis modis geschehen könne. Der erste valor pro $p$ ist, wie Ew. observirt, zwischen 2 und 3, nehmlich $p = 2{,}26618021$, der wahre valor aber ist $p = \frac{\pi}{2l2}$, da ist $\pi = 3{,}14159265$ und $l2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \text{etc.} = 0{,}6931471805$. Alle folgenden valores ipsius $p$ entspringen aus diesem, indem man diesen mit 3, 5, 7, 9, etc. multiplicirt. — — —

Euler.