sunt, die curva, normales omnes in duas partes aequales dividens, wie die innere Figur anzeiget, tricuspidalis ist.

Die aequatio $4n + 5 = 4\square + 4\boxdot + \boxdot$ (allwo $\boxdot$ ein quadratum impar, $\square$ ein quadratum par bedeutet) ist zwar allezeit möglich, man kann aber für $\boxdot$, so eines von den vier quadratis ist, nicht ein jedes pro lubitu annehmen, wie in der aequatione $4\boxdot + \boxdot + \boxdot + \boxdot = 8n + 7$ geschiehet, allwo vor eines von diesen vier quadratis ein jedes quadratum $< 8n + 7$ genommen werden kann.

LETTRE CXXV.

=

EULER à GOLDBACH.

SOMMAIRE. Suite des recherches arithmétiques.

Berlin d. 12. April 1749.

Nunmehr habe ich endlich einen bündigen Beweis gefunden, dass ein jeglicher numerus primus von dieser Form $4n + 1$ eine summa duor. quadr. ist. Es sey $\boxed{2}$ das Zeichen der Zahlen, welche summae duor. quadr. sind, so sind meine Sätze folgende:

I. Si $a = \boxed{2}$ et $b = \boxed{2}$, erit etiam $ab = \boxed{2}$, wovon der Beweis leicht.

II. Si $ab = \boxed{2}$ et $a = \boxed{2}$, erit etiam $b = \boxed{2}$. Hievon ist der Beweis schon schwerer und erfordert einige Sätze.

III. Summa duor. quadr. $aa + bb$, ubi a et b communem divisorem non habeant, nullos alios admittit divisores, nisi qui ipsi sint $\boxed{2}$.

IV. Proposito numero primo $4n+1$, per eum semper $a^{4n}-1$ erit divisibilis, nisi ipse numerus a sit per $4n+1$ divisibilis. Den Beweis hievon habe in den Commentariis Petropolitanis gegeben.

V. Da $a^{4n}-1 = (a^{2n}+1)(a^{2n}-1)$, so ist also entweder $a^{2n}+1$ oder $a^{2n}-1$ per $4n+1$ theilbar. Könnte nun ein einiger Fall angezeigt werden, da nicht $a^{2n}-1$, sondern $a^{2n}+1$ durch $4n+1$ divisibel wäre, weil $a^{2n}+1 = \square 2$, so wäre per N. III bewiesen, dass $4n+1$ eine summa duor. quadr. seyn muss.

VI. *Theorema.* Omnis numerus primus formae $4n+1$ est summa duor. quadr.

Demonstr. Si $4n+1$ non esset $\square 2$, quia $a^{4n}-1$, vel etiam $a^{4n}-b^{4n}$ per $4n+1$ est divisibilis (dummodo neque a neque b sit per $4n+1$ divisibile) nunquam $a^{2n}+b^{2n}$, sed semper $a^{2n}-b^{2n}$ per $4n+1$ esset divisibile. Forent ergo sequentes numeri omnes $2^{2n}-1$, $3^{2n}-2^{2n}$, $4^{2n}-3^{2n}$, $5^{2n}-4^{2n}$, etc. (quamdiu radices sunt minores quam $4n+1$) per $4n+1$ divisibiles. Hoc est hujus progressionis 1, 2^{2n}, 3^{2n}, 4^{2n}, 5^{2n}, ... $(4n)^{2n}$ differentiae forent per $4n+1$ divisibiles. Forent ergo quoque differentiae secundae et tertiae et quartae et tandem differentiae ordinis $2n$, quae sunt constantes, per $4n+1$ divisibiles.

At ex doctrina differentiarum notum est, differentias ordinis $2n$, quae sunt constantes, esse $= 1.2\ 3.4 \ldots . 2n$, qui numerus, cum non sit divisibilis per numerum primum $4n+1$, sequitur non omnes differentias $2^{2n}-1$, $3^{2n}-2^{2n}$, $4^{2n}-3^{2n}$, etc. per $4n+1$ esse divisibiles; dabitur ergo quaedam differentia $a^{2n}-b^{2n}$, quae non erit per $4n+1$ divisibilis, quare cum $a^{4n}-b^{4n} = (a^{2n}+b^{2n})(a^{2n}-b^{2n})$ semper sit per $4n+1$ divisibilis (in serie enim superiori, cujus differentias sum

contemplatus, termini tantum usque ad $(2n+1)^{2n}$ continuantur, ita ut sit a et $b < 2n+1$, ideoque neque a neque b per se sit per $4n+1$ divisibilis, qui casus sunt excepti) necesse est ut hoc casu factor $a^{2n}+b^{2n}$ sit per $4n+1$ divisibilis, qui cum sit $\square 2$, ejus quoque divisorem $4n+1$ summam duor. quadr. esse oportet. Q. E. D.

Dass eine jede Zahl eine summa quatuor vel pauciorum quadratorum sey, kann ich beynahe beweisen; es fehlt mir nehmlich nur noch an einer Proposition, welche dem ersten Ansehen nach keine Schwierigkeit zu haben scheint.

Dieses Zeichen $\square 4$ bedeute eine jegliche Zahl, welche eine Summ von 4 oder weniger quadratis ist, so sind meine Sätze folgende:

I. Si $a = \square 4$ et $b = \square 4$ erit quoque $ab = \square 4$. Hievon ist der Beweis bündig, denn es sey $a = pp+qq+rr+ss$ und $b = xx+yy+zz+vv$, so wird

$ab = (px+qy+rz+sv)^2 + (py-qx \pm rv \mp sz)^2 + (pz \mp qv - rx \pm sy)^2 + (pv \pm qz \mp ry - sx)^2 = \square 4$.

II. Si $ab = \square 4$ et $a = \square 4$, erit etiam $b = \square 4$. Dieses ist der Satz, worauf die ganze Sach beruhet, und den ich noch nicht beweisen kann.

III. *Coroll.* (Dieses Zeichen $\asymp$ soll nach Ew. negationem aequalitatis bedeuten). Si ergo $ab = \square 4$ et $a \asymp \square 4$, tum etiam $b \asymp \square 4$. Si enim esset $b = \square 4$, per II. foret quoque $a = \square 4$ contra hyp.

IV. Si omnes numeri primi essent formae $\square 4$, tunc omnes omnino numeri in hac forma continerentur. Manifestum est ex N. I, unde demonstratio propositi ad numeros tantum primos revocatur.

V. Proposito numero primo quocunque p, semper datur numerus formae $aa+bb+cc+dd$ per p divisibilis, ita ut

nullus numerorum a, b, c, d seorsim per p sit divisibilis. Ich kann nehmlich beweisen, dass es allzeit solche Zahlen $aa+bb+cc+dd$, und das unendlich viel gibt, obschon ich in genere keine davon anzuzeigen vermögend bin. Der Beweis davon ist insbesondere merkwürdig, aber etwas weitläufig und kann auf Belieben den Inhalt eines ganzen Briefes inskünftige abgeben.

VI. Si $aa+bb+cc+dd$ per p est divisibile, quantumvis numeri a, b, c, d sint magni, semper exhiberi potest similis forma $xx+yy+zz+\nu\nu$ per p divisibilis, ita ut singuli numeri x, y, z, ν semisse ipsius p non sint majores.

Demonstr. Erit enim $a \equiv \alpha p \pm x$, $b \equiv \beta p \pm y$, $c \equiv \gamma p \pm z$, $d \equiv \delta p \pm \nu$ atque x, y, z, ν erunt numeri non majores quam $\frac{1}{2}p$. Cum igitur sit $aa+bb+cc+dd \equiv (\alpha\alpha+\beta\beta+\gamma\gamma+\delta\delta)pp \pm 2p(\alpha x+\beta y+\gamma z+\delta\nu)+xx+yy+zz+\nu\nu$ haecque forma per p divisibilis existat, ob duo priora membra jam sponte per p divisibilia, necesse est ut ultimum membrum $xx+yy+zz+\nu\nu$ quoque per p sit divisibile.

VII. Si p est numerus primus ideoque impar, erunt singuli numeri x, y, z, ν minores quam $\frac{1}{2}p$, ideoque

$$xx+yy+zz+\nu\nu < 4 \cdot \tfrac{1}{4}p^2 < p^2.$$

VIII. Si p est numerus primus, certe erit summa quatuor quadratorum vel pauciorum.

Demonstr. Per N. VI datur numerus $aa+bb+cc+dd$ per p divisibilis, ac per N. VII dabitur etiam numerus $xx+yy+zz+\nu\nu$ per p divisibilis, ita ut sit

$$xx+yy+zz+\nu\nu < pp$$

Quodsi jam darentur numeri $\not\equiv \square$, existeret horum numerorum minimus, qui sit $\equiv p$, ita ut sit p minimus eorum numerorum, qui in quatuor quadrata sunt irresolubiles, (hic semper de numeris integris est sermo). Sit igitur

$$xx+yy+zz+\nu\nu \equiv \square \equiv pq,$$

et quia per hyp. $p \not\equiv \square$, foret quoque $q \not\equiv \square$, at $pq < pp$, ideoque $q < p$, ac propterea haberetur numerus q minor quam p, qui esset $\not\equiv \square$, contra hypoth. Nullus ergo datur numerus minimus in quatuor quadrata irresolubilis, ideoque nullus plane datur numerus $\not\equiv \square$, ac per consequens omnis numerus $p \equiv \square$.

Weil ich nicht zweifle, dass diese demonstrationes Ew. nicht gefallen sollten, so bitte dieselben Dero Aufmerksamkeit zu würdigen.

In meinen Umständen ist seit der Zeit nichts veränderliches vorgefallen, als dass ich dieser Tage in einer Lotterie 600 Rthlr. gewonnen, welches also eben so gut ist, als wenn ich dieses Jahr einen Pariser Preis gewonnen hätte.

Euler.