Von der Wahrheit eines andern theorematis bin ich bey weitem nicht so persuadiret, nehmlich dass eine jede Zahl aus dreyen trigonalibus bestehet, oder dass ein jeder numerus hujus formae $8m+3$ eine summa trium quadratorum sey. Ew. haben mir schon vor einigen Jahren, wenn ich mich recht erinnere, gesaget, dass Fermatius selbiges seinem Berichte nach, demonstriren können; zu dergleichen Demonstration aber halte ich die inductiones für unzulänglich, weil man unzählige Exempel pro valoribus m angeben kann, die zwar zutreffen, allein zur Generalität des Satzes nichts contribuiren (als ex. gr. wenn m diese Form hat $bb+bc+cc$). Wenn man aber nur beweisen könnte, dass $(2p-1)^2+42$ allezeit eine summa trium quadratorum sey (ich habe es nur bis auf den casum $p=17$ probiret), so hielte ich davor, dass zur völligen Demonstration des theorematis ein guter Anfang gemacht seyn würde. Indessen sehe ich nicht, wie man es demonstriren will, ohne zugleich eine Methode zu finden, wodurch die tria quadrata selbst angegeben werden können. Aber zu beweisen, dass ein jeder numerus aus dreyen trigonalibus uno affirmativo et duobus negativis bestehet, ist bey weitem nicht so schwer.

Aus den Zeitungen von gelehrten Sachen ist zu ersehen, dass ein gewisser H. Mizler über Ew. Buch von der Musik Anmerkungen gemacht. Weil mir dieselben ganz unbekannt sind, so bitte mir nur mit ein paar Worten zu melden, was Sie davon halten. Die neue Logik des Hn. Knutzen, die ich auch noch nicht gesehen habe, wird in den gel. Z. sehr gerühmet.

Goldbach.

LETTRE CV.

=

EULER à GOLDBACH.

SOMMAIRE Mêmes sujets. Théorèmes de la théorie des nombres.

Berlin d. 6 Mai. 1747.

Der Anmerkung, welche Ew. über die Gleichheit

$$A\ldots.(1-x)(1-x^2)(1-x^3)(1-x^4)\text{ etc.} =$$
$$B\ldots.1-x-x^2+x^5+x^7-\text{etc.}$$

gemacht, dass, wenn

$$C=1-x^2-x^4+x^{10}+x^{14}-x^{24}-x^{30}+\text{etc.},$$

alsdann sey $\frac{C}{B}=(1-x)(1-x^3)(1-x^5)$ etc., erinnere ich mich noch wohl. Ich habe aber weder daraus, noch aus andern Betrachtungen, die Gleichheit zwischen den Formuln A und B richtig darthun können; denn dass $A=B$ und dass in B die Exponenten von x just nach dieser serie 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, etc. fortgehen, habe ich auch nur per inductionem geschlossen, welche ich zwar so weit fortgesetzet, dass ich die Sach für völlig wahr halten kann; allein ich wäre sehr begierig davon eine demon-

strationem directam zu sehen, welche gewiss zu Entdeckung vieler anderer herrlichen Eigenschaften der Zahlen den Weg bahnen würde; bisher ist aber alle meine darauf gewandte Mühe umsonst gewesen. Gleichfalls habe ich bisher auch nicht das gemeldte theorema Fermatianum, dass eine jede Zahl eine summa trium trigonalium sey, demonstriren können, welches freylich darauf beruhet, dass eine jede Zahl von dieser Form $8m+3$ in drey quadrata zertheilet werden könne. Ich habe aber dieses theorema auf folgendes gebracht: Proposito numero quocunque m, ab eo semper ejusmodi numerum trigonalem subtrahere licet, ut residui quadruplum unitate auctum sit numerus primus. Wenn dieses bewiesen werden könnte, so wäre auch jenes ausser Zweifel gesetzt. Von diesem aber will ich der Deutlichkeit halber etliche Exempel hersetzen:

m — trig.	resid.	4 res. + 1
1 — 0	1	5 pr.
1 — 1	0	1 pr.
2 — 0	2	9 *n. pr.*
2 — 1	1	5 pr.
3 — 0	3	13 pr.
3 — 1	2	9 *n. pr.*
3 — 3	0	1 pr.

m — trig.	resid.	4 res. + 1
4 — 0	4	17 pr.
4 — 1	3	13 pr.
4 — 3	1	5 pr.
5 — 0	5	21 *n. pr.*
5 — 1	4	17 pr.
5 — 3	2	9 *n. pr.*
6 — 0	6	25 *n. pr.*
6 — 1	5	21 *n. pr.*
6 — 3	3	13 pr.
6 — 6	0	1 pr.

m — trig.	resid.	4 res. + 1
7 — 0	7	29 pr.
7 — 1	6	25 *n. pr.*
7 — 3	4	17 pr.
7 — 6	1	5 pr.
8 — 0	8	33 *n. pr.*
8 — 1	7	29 pr.
8 — 3	5	21 *n. pr.*
8 — 6	2	9 *n. pr.*
9 — 0	9	37 pr.
9 — 1	8	33 *n. pr.*
9 — 3	6	25 *n. pr.*
9 — 6	3	13 pr.

Bisher triffts immer zu, dass zum wenigsten ein numerus primus herauskommt; und da in grösseren Zahlen immer mehr casus vorkommen, so ist sehr wahrscheinlich, dass sich unter denselben zum wenigsten immer ein primus befinde, oder ein solcher compositus, der ein Quadrat, oder in zwey quadrata resolubel ist. Es ist auch eben zur Demonstration des ersteren nicht nöthig, dass bey dem letztern sich unter den 4 resid. + 1 ein numerus primus befinde. Wenn darunter nur entweder ein quadratum vorkommt, oder eine Zahl per nullum hujusmodi numerum $4p-1$ divisibilis, so kann daraus die Demonstration des ersteren hergeleitet werden. Der Grund davon beruhet hierauf: ich kann nun beweisen, dass

I. Omnem numerum primum hujus formae $4n+1$ esse summam duorum quadratorum.

II. Omnem quoque numerum non primum formae $4n+1$, dummodo nullum habeat divisorem formae $4p-1$, esse summam duorum quadratorum.

Es sey also $4n+1$ vel primus vel saltem non habens divisorem formae $4p-1$, so ist $4n+1$ und folglich auch ejus duplum $8n+2$ summa duorum quadratorum. Wenn also $8m+3 = 8n+2+aa$, so ist $8m+3$ in tria quadrata resolubel. Es wird also $8m+1 = 8n+aa$; man setze $a = 2x+1$, so wird $8m = 8n+4xx+4x$ und $n = m-\frac{1}{2}(xx+x)$. Denotante ergo m numerum quemcunque, wenn man nur immer von m einen solchen numerum trigonalem subtrahiren kann, dass der Rest 4 mal genommen + 1 keinen divisorem formae $4p-1$ hat, so kann $8m+3$ in drey quadrata resolvirt werden. Dass aber eine jede Primzahl von dieser Form $4n+1$ allzeit eine

summa duorum quadratorum sey, dafür habe ich nach langer Mühe endlich folgende Demonstration gefunden, welche sich auf verschiedene Präliminarsätze gründet, so zwar gemeiniglich für wahr angenommen werden, wovon ich doch gleichwohl noch keine gültige Demonstration gesehen, und also diese zu suchen nöthig gehabt habe.

Theor 1. Productum ex duobus numeris, quorum uterque est summa duorum quadratorum, est quoque summa duorum quadratorum.

Demonst. Sint $aa+bb$ et $cc+dd$ duo numeri propositi, erit productum $aacc+aadd+bbcc+bbdd = (ac+bd)^2+(ad-bc)^2 = (ac-bd)^2+(ad+bc)^2$, ergo duplici modo summa duorum quadratorum. — Diese Demonstration ist zwar gemein, nicht aber die folgenden.

Theor. 2. Si summa duorum quadratorum $aa+bb$ (existentibus a et b numeris inter se primis) fuerit divisibilis per numerum primum formae $pp+qq$, tum etiam quotus, ex divisione resultans, erit summa duorum quadratorum. (Dieses theorema folget nicht aus dem vorigen nothwendig, denn man würde sich betrügen, wenn man hieraus: productum ex duobus numeris paribus est numerus par, schliessen wollte: ergo si numerus par fuerit divisibilis per numerum parem, quotus quoque erit numerus par. Wie kann man nun wissen, dass diese Art zu schliessen hier richtig ist? Dahero ist meines Erachtens folgende Demonstration nöthig.)

Demonstr. Quia $aa+bb$ est divisibilis per $pp+qq$, erit quoque $(aa+bb)pp = aapp+bbpp$ divisibile, at $aa(pp+qq)$ quoque est divisibile per $pp+qq$, ergo etiam differentia $bbpp-aaqq$ h. e. $(bp+aq)(bp-aq)$ erit per $pp+qq$ divisibile. Hinc ob $pp+qq$ numerum primum, erit vel

$bp+aq$ vel $bp-aq$ divisibile per $pp+qq$. Sit ergo $bp \mp aq = mpp+mqq$, fietque $b = mp + \frac{mqq \pm aq}{p}$. Cum igitur $mqq \pm aq$ per p divisibile esse debeat, at q et p sint necessario numeri inter se primi (alioquin $pp+qq$ non foret primus), necesse est ut $mq \pm a$ divisibile sit per p. Fiat ergo $mq \pm a = np$, erit $\pm a = np - mq$ et $b = mp+nq$. His autem valoribus substitutis prodit $aa+bb = (mm+nn)(pp+qq)$ et $\frac{aa+bb}{pp+qq} = mm+nn$. Q. E. D.

Theor. 3. Si summa duorum quadratorum $aa+bb$ (a et b existentibus perpetuo numeris inter se primis) divisibilis esset per numerum x, qui non sit summa duorum quadratorum, tum quotus vel non erit summa duorum quadratorum, vel certe factorem haberet qui non erit summa duorum quadratorum.

Demonstr. Sit quotus z et ob $\frac{aa+bb}{x} = z$, erit $\frac{aa+bb}{z} = x$. Jam si z esset primus formae $pp+qq$, tum quoque x foret ejusdem formae contra hyp. Si z esset productum ex pluribus hujusmodi primis $(pp+qq)(rr+ss)(tt+uu)$, tum ob $\frac{aa+bb}{pp+qq} = cc+dd$, $\frac{cc+dd}{rr+ss} = ee+ff$ et $\frac{ee+ff}{tt+uu} = gg+hh = \frac{aa+bb}{z}$, foret quoque $x = gg+hh$ contra hyp. Quare quotus z neque primus erit formae $pp+qq$, neque productum ex aliquot ejusmodi primis; ideoque necessario vel z non erit summa duor. quadr., vel factorem habebit qui non erit summa duor. quadr. Q. E. D.

Theor. 4. Summa duor. quadr. inter se primorum $aa+bb$ dividi nequit per ullum x, qui non ipse sit summa duor. quadratorum.

Demonstr. Ponamus x non esse summam duor. quadr., sitque $a = mx \pm c$, $b = nx \pm d$, semperque m et n ita capi poterunt ut fiat $c < \frac{1}{2}x$ et $d < \frac{1}{2}x$. Cum autem $aa + bb$ ponatur divisibile per x, erit quoque $cc + dd$ per x divisibile, et quia $cc + dd < \frac{1}{2}xx$, quotus erit $< \frac{1}{2}x$, ideoque dabitur numerus z non summa duor. quadr., per quem $cc + dd$ quoque erit divisibilis (Theor. 3). Sit iterum $c = mz \pm e$ et $d = nz \pm f$, erit $e < \frac{1}{2}z$ et $f < \frac{1}{2}z$, ideoque $ee + ff < \frac{1}{2}zz$ divisibile per z; unde quotus (per quem $ee + ff$ itidem divisibile existit) $< \frac{1}{2}z$, qui vel ipse erit *non summa* duor. quadr., vel ejusmodi habebit factorem. Dabitur ergo *non summa duor. quadr.* $< \frac{1}{2}z$ divisor ipsius $ee + ff < \frac{1}{2}zz$, sicque tandem deveniretur ad numerum *non summam duor. quadr.* minimum, puta 3, qui foret divisor summae duor. quadr $gg + hh < \frac{1}{2}g$, quod cum sit absurdum, sequitur summam duorum quadr. $aa + bb$ nullum admittere divisorem x, qui non sit ipse summa duor. quadr. Q. E. D.

Coroll. 1. Omnis ergo divisor summae duor. quadr. inter se primorum ipse est summa duor. quadr., loquor autem de ejusmodi summis duor. quadr. $aa + bb$ quorum radices a et b sunt numeri inter se primi, nam si esset v. gr. $a = mx$ et $b = nx$, tum $aa + bb$ utique per quemvis numerum x divisibilis esse posset.

Coroll. 2. Qui ergo numerus x in integris non est summa duor. quadr. idem nec in fractis poterit esse summa duor. quadr. Sit enim $x = \frac{pp}{qq} + \frac{rr}{ss} = \frac{ppss+qqrr}{qqss}$, foret $qqss = \frac{ppss+qqrr}{x}$, ideoque x divisor summae duor. quadratorum

$ppss + qqrr$, ergo x quoque esse debet summa duor. quadr. in integris. Hievon hatte ich lange eine Demonstration umsonst gesucht, aber diese erst neulich gefunden, welche, wie ich glaube, zu vielen andern Sachen führen kann.

Theor. 5. Si $4n + 1$ fuerit numerus primus, tum certo erit summa duor. quadr.

Demonstr. Si enim $4n + 1$ sit numerus primus, demonstravi hanc formulam $a^{4n} - b^{4n}$ quicunque numeri pro a et b ponantur, semper fore divisibilem per $4n + 1$. Erit ergo vel $a^{2n} + b^{2n}$ vel $a^{2n} - b^{2n}$ per $4n + 1$ divisibile. At semper innumeri dantur casus, quibus formula $a^{2n} - b^{2n}$ non est divisibilis per $4n + 1$; iis ergo casibus haec formula $a^{2n} + b^{2n}$ erit per $4n + 1$ divisibilis. At $a^{2n} + b^{2n}$ est summa duor. quadr., ergo etiam quivis ejus divisor $4n + 1$. Q. E. D.

Theor. 6. Qui numerus a duplici modo est summa duor. quadr., ille non est primus.

Demonstr. Sit enim $a = pp + qq = rr + ss$, ponatur $p = r + x$ et $q = s - y$ erit $pp + qq = rr + 2rx + xx + ss - 2sy + yy = rr + ss$, ergo $2sy = xx + yy + 2rx$ et $s = \frac{xx+yy+2rx}{2y}$, hinc

$$a = rr + ss = \frac{(xx+yy)^2 + 4rx(xx+yy) + 4rrxx}{4yy} + rr$$
$$= \frac{(xx+yy)(xx+yy+4rx+4rr)}{4yy}.$$

Consequenter numerus a necessario duos ad minimum habet factores, quorum uterque est summa duor. quadr. Q. E. D.

Das theorema: Omnem numerum in quatuor quadrata esse resolubilem, dependiret hievon:

Omnem numerum hujus formae $4m + 2$ semper discerpi posse in duas hujusmodi partes: $4x + 1$ et

$4y + 1$ quarum neutra divisorem habeat formae $4p - 1$.

welches ich noch nicht demonstriren kann, aber doch nicht schwer scheinet. — Denn alsdann ist sowohl $4x+1$ als $4y+1$ summa duor. quadr. und folglich $4m+2$ summa 4 quadr. Dahero auch ejus duplum $8m+4$ und hujus quadrans $2m+1$ und also omnis numerus impar, woraus die Folge leicht auf alle numeros extendirt wird.

Des Hn. Mitzlers critique über meine Music habe ich nicht gesehen, ausser was davon in den gel. Zeitungen stehet, woraus ich geschlossen, dass dieselbe meistentheils übel gegründet ist, indem der Auctor meine Gedanken nicht genugsam eingesehen. An des Hn. Prof. Knutzen Logic habe ich eben nicht viel Sonderbares finden können; zum wenigsten kommt sie derjenigen bei weitem nicht bey, welche der H. Prof. Segner in Göttingen herausgegeben. Dieses Jahr hat mir die Akademie zu Paris wiederum die Hälfte des Preises zuerkannt, welche 2000 livr. beträgt.

M. Buffon in Paris hat eine neue Art von Brennspiegeln erfunden, vermittelst welcher er in einer Distanz von 200 Schuh Holz in Brand gestecket, und diese Distanz kann nach Belieben noch vermehrt werden.

Euler.

LETTRE CVI.*)

=

GOLDBACH à EULER.

SOMMAIRE. Réponse à la précédente Machine à mouvement perpétuel d'Orffyrei.

St Petersburg d. 2 Juni 1747.

Für die mir communicirten theoremata bin ich Ew. sehr verbunden. Das merkwürdigste darunter halte ich, dass Sie meinen, es sey nicht schwer $4m+2$ in zwey solche Theile $4x+1$ und $4y+1$ zu resolviren, welche keinen divisorem hujus formae $4p-1$ haben. Ich kann das problema: numerum $8m+3$ in tria quadrata resolvere auch auf dieses reduciren: Datis duobus numeris n et p, invenire tertium x hujus naturae, ut $2+8n+8px-4xx-4x$ fiat summa duorum quadratorum, da dann vor x eine solche functio ex n et p composita gefunden werden soll, welche unter andern diese seltsame Eigenschaften habe, dass sie in allen

*) Le premier feuillet de la lettre originale étant égaré, le commencement a été suppléé du livre des minutes.