pesci potest in duos factores, nempe duobus modis (1) 1.65, (2) 5.13, est igitur aggregatum duor. quadr. (1) $1+64$, (2) $16+49$.

Similiter 25 est numerus hujus formae $4n+1$ nec dividi potest per numerum hujus formae $4m-1$, igitur cum dupliciter resolvi possit in duos factores, nempe (1) in 1 et 25, (2) in 5 et 5, erit dupliciter summa duorum quadratorum (1) $0+25$, (2) $9+16$.

Similiter numerus 625 ejusdem naturae tripliciter resolvitur in duos factores (1) 1.625, (2) 5.125, (3) 25.25, ergo tripliciter est summa duor. quadr. (1) 0^2+25^2, (2) 7^2+24^2, (3) 15^2+20^2.

Numerus 493 ejusdem naturae duobus modis resolvi potest in duos factores (1) 1.493, (2) 17.29, ergo duobus modis est summa duor. quadr. (1) 3^2+22^2, (2) 13^2+18^2 etc.

Uebrigens habe ich zwey Methoden, wenn die aequatio $emq-q-m=aa$ in einem casu q possibilis ist, innumeros alios casus pro aequatione $emn-m-n=bb$ zu finden, nämlich si fiat

I. $q-2ak+(em-1)kk=n$,

II. $((em-1)h+1)^2q-hm((em-1)h+2)=n$

ubi h et k sint numeri quicunque, modo n fiat integer, deren Wahrheit per ipsam substitutionem alsofort demonstriret wird.

Goldbach.

LETTRE LXXIX.

EULER à GOLDBACH.

SOMMAIRE. Suite des recherches arithmétiques. Problème de la courbe catoptrique. Equation différentielle à intégrer.

Berlin d. 16 Februar 1745.

— — Dass diese Formul $emn-m-n$ nimmer ein Quadrat seyn könne, wenn e entweder eine solche Zahl $4k$, oder eine solche $8k-1$ ist, habe ich nur aus einer Induction geschlossen. Diese Observation erhält aber durch Ew. Entdeckung einen weit grössern Grad der Gewissheit. Denn dadurch wird unwidersprechlich dargethan, dass so oft entweder e oder $e-1$ ein divisor ist von $cc+1$, für m et n allezeit solche Zahlen gefunden werden können, dass $emn-m-n$ ein Quadrat wird. Weil nun weder $4k$ noch $8k-1$ immer hierin Platz finden können, so kann auf diese Art weder für $e=4k$, noch für $e=8k-1$ die Formul $emn-m-n$ zu einem Quadrat gebracht werden. Um

aber die Demonstration vollkommen zu machen, so müsste man auch die propositionem conversam beweisen können, dass so oft $emn - m - n$ ein Quadrat seyn kann, auch entweder e oder $e - 1$ ein divisor sey von einer solchen Zahl $xx + 1$. So lang also dieses nicht erwiesen ist, so lang kann man auch nicht behaupten, dass der obige Satz völlig bewiesen worden, ob man gleich daran gar keine Ursach zu zweifeln hat. Es gibt in der Arithmetik eine grosse Menge solcher Sätze, an welchen Niemand zweifelt, ungeacht man dieselben nicht demonstriren kann. Ich habe zum Ex. diesen Satz noch nirgend bewiesen gefunden: qui numerus in integris non est summa duorum quadratorum, eundem ne in fractis quidem esse posse summam duorum quadratorum. Um dieses zu beweisen, müsste man zeigen, dass, wenn ann einer summa duorum quadratorum gleich ist, auch allzeit a eine summa duorum integrorum quadratorum seyn müsse. Gleichergestalt ist leicht zu demonstriren, dass das Product ex binis summis duorum quadratorum, auch eine summa duorum quadratorum sey. Hieraus erhellet aber noch nicht, dass, wenn eine summa duorum quadratorum per summam duorum quadratorum dividirt wird, der quotus auch eine summa duorum quadratorum seyn müsse, woran doch Niemand zweifelt. Es ist auch meines Bedünkens noch nicht erwiesen, dass eine summa duorum quadratorum inter se primorum keine andere divisores haben könne, nisi qui sint ipsi duorum quadratorum summae. Eine gleiche Bewandniss hat es auch mit dieser Proposition: Omnem numerum primum hujus formae $4n + 1$ semper esse summam duorum quadratorum, idque unico modo. Wenn man nun dieses voraussetzt, so liessen sich Ew. theoremata leicht erweisen. Denn, wenn $4n + 1$ keinen divisorem hat formae

$4m - 1$, so müssen alle factores von dieser Form $4m + 1$ und folglich summae duorum quadratorum seyn. Es ist aber generaliter $(aa + bb)(cc + dd) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$ und also duplici modo in duo quadrata resolubile. Hernach lässt sich auch leicht erweisen, quod, si quis numerus duplici modo in duo quadrata fuerit resolubilis, eum non esse primum. Sit enim $N = aa + bb = cc + dd$, erit $N = \frac{((a-c)^2+(b-d)^2)((a+c)^2+(b-d)^2)}{4(b-d)^2}$. Ferner hat auch dieser Satz seine Richtigkeit: Si numerus $4n + 1$ unico modo in duo quadrata resolvi possit, tum certo erit numerus primus; sin autem $4n + 1$ nullo modo fuerit summa duorum quadratorum, tum non erit primus, sed factores habebit formae $4m - 1$ vel duos, vel 4, vel 6, etc. At si $4n + 1$ pluribus modis fuerit summa duorum quadratorum, tum quoque binos pluresve habebit factores formae $4m + 1$. Und aus diesem Grunde ist nicht schwer, sehr grosse Zahlen $4n + 1$ zu untersuchen, ob dieselben primi sind, oder nicht?

Gleich wie ich bewiesen habe, dass alle divisores primi hujus formae $a^2 + b^2$ in dieser Expression $4n + 1$ enthalten sind, also kann ich auch demonstriren, dass alle divisores von $a^4 + b^4$ in dieser Form $8n + 1$, und generaliter dass alle divisores von $a^{2^m} + b^{2^m}$ in dieser Form $2^{m+1}n + 1$ enthalten sind. Folgende theoremata kann ich auch rigorose beweisen:

I. Si $a^m - b^m$ fuerit divisibilis per numerum primum $2n + 1$, atque p sit maximus communis divisor numerorum m et $2n$, tum quoque $a^p - b^p$ per $2n + 1$ divisibilis erit.

II. Si haec formula $af^n - bg^n$ fuerit divisibilis per numerum primum $mn + 1$, tum quoque $a^m - b^m$ per $mn + 1$

erit divisibile. Si ergo pro f et g ejusmodi numeros invenire liceat, ut $af^n - bg^n$ sit divisibile per $mn+1$, tum formula $a^m - b^m$ necessario erit per $mn+1$ divisibilis.

Ich bin letztens auf dieses problema gefallen: (Fig. 10) Circa datum punctum radians R curvam describere ejusmodi, ut singuli radii ex R egressi post duplicem reflexionem in M et N in ipsum punctum R revertantur. Es gibt ausser der Ellipse, alterum focum in R habente, noch unendlich viel andere Linien quaesito satisfacientes, sowohl algebraicae als transcendentes; und dieses problema däucht mich eines von den schwersten in hoc genere zu seyn.

Haec aequatio

$$ay\,dy + y\,dx\,(3ax+b) + dx\,(ax^3 + bxx + cx + f) = 0$$

potest separari et integrari.

Euler.

LETTRE LXXX.

=

GOLDBACH à EULER.

SOMMAIRE. Réponse aux deux derniers articles de la précédente.

St. Petersburg d. 29 Mai 1745.

Die integrationem aequationis

$$ay\,dy + y\,(3ax+b)\,dx + (ax^3 + bxx + cx + f)\,dx = 0$$

halte ich vor sehr leicht, indem ich alsofort gefunden $y = -xx + \beta x + \gamma$, ubi $a\alpha\beta^3 + 2ab\beta\beta + (ac+bb)\beta + bc = af$ et $\gamma = \frac{-a\beta\beta \mp b\beta - c}{a}$.

Was das andere problema betrifft, so wird die curva nachfolgende proprietates haben:

1. muss (Fig. 11), posita $AB = x$, $BC = y$, $HA = a$, $AG = b$, y eine solche functio ipsius x seyn, dass positis $x = -a$ et $x = b$, $y = 0$ werde.

2. Weil die pars axis inter radium incidentem AC et radium reflexum CD intercepta, nehmlich AD per x et y