$\frac{\sqrt{(4f-mm)}}{\sqrt{(emm+1)}}$, können gleichfalls die numeri quaesiti P et Q in rationalibus angegeben werden; imgleichen wenn $QQ = 4fvv + 2mv - emm$ gefunden werden kann, so wird $1 + 4ef = \frac{(4fv+m)^2 - 4fQQ}{mm} = \frac{(emm-v)^2 + eQQ}{vv}$, und endlich, weil der numerus primus $1 + 4ef =$ ist duobus quadratis $aa + bb$, quae in quocunque casu determinari possunt, so ist genug, wenn man nur einen numerum rationalem k finden kann hac lege, ut $aa(e + kk) + bb(e - kk)$ fiat quadratus, da es alsdann nicht schwer ist die numeros quaesitos P et Q zu finden, denn es wird

$$aa + bb = \frac{(hh+1)^2 aa}{4hh} + \frac{ekk(hh-1)^2 aa}{hh(e-kk)^2}$$

si sumatur

$$h = \frac{b(e-kk) \pm \sqrt{(aa(e+kk)^2 + bb(e-kk)^2)}}{a(e+kk)}.$$

Ferner ist auch diese Proprietät merkwürdig, ungeachtet ich mich um deren Demonstration nicht bemühet: Si quadratum aliquod divisum per numerum primum p hujus formae $4n+1$, relinquat numerum r, dabitur etiam aliud quadratum, quod divisum per eundem numerum p, det residuum $p - r$.

Imgleichen numerus primus $4n+1$, dividens numeros quadratos quoscunque, tot relinquere potest diversa residua quot $2n$ continet unitates, als z. Ex. wenn $n = 1$, so kann der divisor 5 nur zwey residua nachlassen, nehmlich 1 und 4; wenn $n = 3$, so lässet der divisor 13, dividens quadratos, sex residua, nehmlich 1, 3, 4, 9, 10, 12, et ita reliqui.

Goldbach.

LETTRE CLVII.

=

Euler à Goldbach.

Sommaire. Même sujet. Réponse à la précédente.

Berlin d. 17. Mai 1755.

Ew. Betrachtungen über das theorema, dass die Zahl $1 + 4ef$, so oft sie ein numerus primus ist, immer in dieser Form $P^2 + eQ^2$ enthalten sey, habe ich mit dem grössten Vergnügen zu ergründen gesucht und darin sehr wichtige Kunstgriffe wahrgenommen; nur ist es schad, dass dieselben noch so weit von einer vollständigen Demonstration entfernt sind. Doch ist es schon von keinem geringen Nutzen, dass, da man von der Wahrheit des theorematis versichert ist, auch alle die daraus hergeleiteten Formuln gewiss resolvirt werden können, welches sonsten sehr schwer fallen würde. Aus allen Bemühungen, die ich hierüber angewandt, deucht mich so viel sicher schliessen zu können, dass man niemals

eine solche Demonstration finden wird, aus welcher zugleich ex dato numero primo $1+4ef$, die quadrata P^2 und Q^2 selbst angegeben werden könnten; sondern man muss sich nur mit einer solchen begnügen, welche die Möglichkeit, dass $1+4ef=P^2+eQ^2$, beweiset, ohne den modum anzuzeigen, wie diese Resolution wirklich anzustellen. Denn da dieselbe nur alsdann möglich ist, wenn $1+4ef$ ein numerus primus ist, so sehe ich nicht ab, wie man diese nothwendige Bedingung in Betrachtung ziehen könnte. Es ist also eine verlorne Mühe, die numeros P et Q generaliter durch e und f bestimmen zu wollen: denn wenn solches möglich wäre, so müssten auch die Zahlen P und Q gefunden werden können, wenn auch $1+4ef$ kein numerus primus wäre, welches doch gewiss öfters unmöglich ist.

Es ist mir endlich wohl gelungen zu beweisen, dass $1+4f=PP+QQ$, so oft $1+4f$ ein numerus primus ist; allein der Beweis hilft mir im geringsten nichts, um einen solchen numerum primum $1+4f$ würklich in zwey quadrata zu resolviren.

Neulich habe ich auch die Beweise zu Stande gebracht, dass $1+8f=1+4.2f=PP+2QQ$ und $1+12f=1+4.3f=PP+3QQ$, so oft nehmlich diese Zahlen $1+8f$ und $1+12f$ numeri primi sind. Doch habe ich bisher noch nicht weiter gehen können.

Ich sehe aber, dass sich diese Formuln noch weiter erstrecken, denn es ist nicht nur $1+8f=PP+2QQ$, sondern auch $3+8f=PP+2QQ$, wenn es numeri primi sind. Hernach ist auch $7+12f=PP+3QQ$. Hernach, wenn $e=5$ genommen wird, so hat man diese theoremata $1+20f=PP+5QQ$, $9+20f=PP+5QQ$, welche ich aber nicht beweisen kann. Vielleicht aber, wenn auch diese

Fälle mit in Betrachtung gezogen werden, findet man etwas eher Mittel, zu einer allgemeinen Demonstration zu gelangen.

Das theorema, dass wenn ein quadratum per numerum primum $p=1+4n$ getheilt, das residuum r lässt, ein anderes Quadrat das residuum $p-r$ zurücklassen müsse, habe ich schon lang bewiesen. Denn wenn $1+4n$ numerus primus et a numerus datus, so können immer unendlich viel Zahlen $aa+xx$ gefunden werden, qui per $1+4n=p$ sint divisibiles; wenn also aa per p divisum r zurücklässt, so muss xx, $p-r$ zurücklassen.

Ew. ist der Beweis bekannt, dass $a^4\pm b^4\neq p^4$. Neulich bin ich auch mit dem Beweis zu Stande gekommen, dass $a^3\pm b^3\neq p^3$; weiter kann ich aber auch nicht kommen. Fermat hat aber nicht nur dies bewiesen, sondern auch dass $a^5\pm b^5\neq p^5$, $a^7\pm b^7\neq p^7$ und generaliter dass $a^n\pm b^n\neq p^n$, exceptis casibus $n=1$ et $n=2$. Allem Ansehn nach kommt es hier auf einen besondern Einfall an, und so lang man nicht darauf kommt, ist alle Arbeit vergebens. Ohne Zweifel wird man darauf sehen müssen, dass a^5+b^5 ausser $a+b$ keine andere divisores primos haben kann, als hujus formae $10m+1$, welches ich bewiesen habe.

Euler.