

minores, loco  $n$  positi, reddunt  $2^n - 1$  primum\*). Potest vero  $2^{11} - 1$  dividi per 23,  $2^{23} - 1$  per 47, et  $2^{85} - 1$  per 167. Ratio hujus fundata est hoc theoremate non ineleganti:  $2^n - 1$  semper potest dividi per  $n + 1$ , siquidem  $n + 1$  fuerit numerus primus. Sic  $2^{22} - 1$  dividi potest per 23. Saepe etiam  $2^{\frac{n}{2}} - 1$ , nec non  $2^{\frac{n}{4}} - 1$  etc. per  $n + 1$  dividi possunt, et ex hoc investigatio casuum, quibus  $2^n - 1$  est numerus primus, non est difficilis. Vale atque fave Tibi obstrictissimo

Leonh. Euler.

---

\*) Euler oublie le nombre 37; dans la lettre 5<sup>ème</sup>, page 23, il fait observer lui-même que  $2^{52} - 1$  est divisible par 223.

---

Si  $p$  est un nombre premier de la forme  $2^n - 1$ , alors  $p$  divise  $2^{\frac{p-1}{2}} - 1$ . Cela signifie que  $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . Soit  $k = \frac{p-1}{2}$ . Alors  $2^k \equiv 1 \pmod{p}$ . Si  $p$  est impair, alors  $k$  est pair. Si  $p$  est pair, alors  $k$  est impair. Dans tous les cas,  $2^k \equiv 1 \pmod{p}$ .

Si  $p$  est un nombre premier de la forme  $2^n - 1$ , alors  $p$  divise  $2^{\frac{p-1}{2}} - 1$ . Cela signifie que  $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . Soit  $k = \frac{p-1}{2}$ . Alors  $2^k \equiv 1 \pmod{p}$ . Si  $p$  est impair, alors  $k$  est pair. Si  $p$  est pair, alors  $k$  est impair. Dans tous les cas,  $2^k \equiv 1 \pmod{p}$ .

## LETTRE XVI.

---

GOLDBACH à EULER.

SOMMAIRE. Rectification d'une formule de la lettre 14<sup>ème</sup>.

---

Moscoue d.  $\frac{6}{17}$  Dec. 1751.

Ante omnia mihi emendanda est aequatio in superioribus litteris meis male descripta, scribendum enim erat, in quo-cunque casu numerorum  $p$  et  $n$  aequatio (A)  $(1 - \nu) \nu dz = (n + p + 1) z \nu d\nu + n(1 - z) d\nu$  est integrabilis, eodem casu aequationem (B)  $(1 - x^{\frac{1}{n}})^p dx = dy$  esse integrabilem, id quod instituto examine deprehendes.

Altera aequatio (C)  $x^{\pm\frac{1}{n+1}} dx - y^2 dx = dy$  simili modo transmutatur in (D)  $dz - \nu^2 dz \pm 2n\nu z^{-1} dz = d\nu$ . Quomodo vero separatio variabilium in aequatione (C) vel (D) pendeat a termino generali seriei, cuius lex progressio-nis est  $A + (2m + 1) B = C$ , non video. De reliquis in posterum. Vale.

Goldbach.

---