

n°175 p41 (début)

Pour tout $n \in \mathbb{N}^*$, l'entier $M_n = 2^n - 1$ est un nombre de Mersenne.

1) les premiers nombres de Mersenne sont:

$$\begin{array}{ll} M_1 = 2^1 - 1 & M_1 = 1 \\ M_2 = 2^2 - 1 & M_2 = 3 \\ M_3 = 2^3 - 1 & M_3 = 7 \\ M_4 = 2^4 - 1 & M_4 = 15 \end{array}$$

2) Pour tout entier a différent de 1 et pour tout $n \in \mathbb{N}$, $n \geq 2$ la somme de termes consécutifs d'une suite géométrique de premier terme 1 et de raison " a " s'écrit:

$$1 \times \frac{1-a^n}{1-a} = 1 + a + a^2 + \dots + a^{n-1}$$

$$1-a^n = (1-a)(1+a+a^2+\dots+a^{n-1})$$

En multipliant les deux membres par -1 , on a:

$$\underline{a^n - 1 = (a-1)(1+a+a^2+\dots+a^{n-1})} \quad \text{pour tout } a \in \mathbb{Z}, a \neq 1$$

Si $a^n - 1$ est premier alors il n'a qu'une seule décomposition possible:

$$a^n - 1 = 1 \times (a^n - 1)$$

ce qui donne donc deux possibilités:

$$\begin{cases} 1+a+a^2+\dots+a^{n-1} = 1 \\ a-1 = a^n - 1 \end{cases} \quad \text{avec } a \neq 1$$

ou bien

$$\begin{cases} 1+a+a^2+\dots+a^{n-1} = a^n - 1 \\ a-1 = 1 \end{cases} \quad \text{avec } a \neq 1$$

la première possibilité est impossible car elle donne $a-1 = a^n - 1$ et $a \neq 1$

Il reste donc la deuxième possibilité qui donne

$$a-1=1$$

$$\text{Donc } \underline{a=2}$$

3) Pour tout $n \in \mathbb{N}$, $n \geq 2$ on a $M_n = 2^n - 1$
et $M_d = 2^d - 1$ avec $d \in \mathbb{N}^*$

Si d divise n , alors il existe $k \in \mathbb{Z}$ tel que $kd = n$

Montrons qu'alors M_d divise $M_n = M_{kd} = 2^{kd} - 1$

$$M_{kd} = (2^d)^k - 1$$

$$M_{kd} = (2^d - 1)(1 + 2^d + (2^d)^2 + \dots + (2^d)^{k-1})$$

$$M_{kd} = M_d \times (1 + 2^d + (2^d)^2 + \dots + (2^d)^{k-1})$$

Comme $(1 + 2^d + (2^d)^2 + \dots + (2^d)^{k-1}) \in \mathbb{Z}$ donc $\underline{M_d \text{ divise } M_{kd} = M_n}$

n°175 p44 (fin)

- 4) Si n est composé, alors il existe un entier $d \neq 1$ tel que d divise n .

D'après la question 3) si d divise n alors M_d divise M_n .
Or $d \neq 1$ donc $M_d \neq 1$.

M_n a comme diviseur M_d qui est différent de 1.
Donc M_n est composé.

- 5) la contraposée de "si p alors q " est "si non q alors non p ".

Donc la contraposée de "si n est composé alors M_n est composé" est:

"si M_n est premier alors n est premier".

la réciproque étant:

"si n est premier alors M_n est premier".

Cette réciproque est fautive:

contre-exemple: $M_{11} = 2^{11} - 1 = 2047$

$$M_{11} = 23 \times 89$$

$n=11$ est premier mais M_{11} est composé.

- 6) Supposons que $a = bq + r$ avec $0 \leq r < b$
Montrons que $2^a - 1 = (2^b - 1)q' + (2^r - 1)$
avec $0 \leq 2^r - 1 < 2^b - 1$

$$\begin{aligned} \text{On a: } 2^a - 1 &= 2^{bq+r} - 1 \\ 2^a - 1 &= 2^{bq} \times 2^r - 1 \\ 2^a - 1 &= (2^{bq} - 1 + 1) \times 2^r - 1 \\ 2^a - 1 &= (2^{bq} - 1) \times 2^r + 2^r - 1 \\ 2^a - 1 &= ((2^b)^q - 1) \times 2^r + 2^r - 1 \end{aligned}$$

En utilisant la somme de termes consécutifs d'une suite géométrique:

$$2^a - 1 = ((2^b - 1)(1 + (2^b) + (2^b)^2 + \dots + (2^b)^{q-1}) \times 2^r + 2^r - 1$$

$$2^a - 1 = (2^b - 1) \times [(1 + (2^b) + (2^b)^2 + \dots + (2^b)^{q-1}) \times 2^r] + 2^r - 1$$

$$\text{Posons } q' = [(1 + (2^b) + (2^b)^2 + \dots + (2^b)^{q-1}) \times 2^r]$$

Comme $2, b, q$ et r sont des entiers, alors $q' \in \mathbb{Z}$

$$\text{On a donc } 2^a - 1 = (2^b - 1) \times q' + 2^r - 1 \quad \text{avec } q' \in \mathbb{Z}$$

C'est bien la relation de division euclidienne de $2^a - 1$ par $2^b - 1$ car on a

$$\begin{aligned} 0 &\leq r < b \\ 2^0 &\leq 2^r < 2^b \\ 1 &\leq 2^r - 1 < 2^b - 1 \\ 0 &\leq 2^r - 1 < 2^b - 1 \end{aligned}$$