

TD 18: Arithmétique dans $\mathbb{Z}$

Exercice 4: Nombres de Fermat

1. Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ premier

Supposons $m = pq$ avec q impair > 1
 p puissance de deux

$$\begin{aligned} \text{on a alors } 2^m + 1 &= (2^p)^q + 1^q \\ &= \underbrace{(2^p + 1)}_{1 < \dots < 2^m + 1} \sum_{i=0}^{q-1} (2^p)^i (-1)^{q-1-i} \end{aligned} \quad \checkmark$$

$\in \mathbb{Z}$

Donc $(2^p + 1) \mid (2^m + 1)$.

et c'est un diviseur strict car

Cas $q \neq 1$:

$$1 < 2^p + 1 < 2^m + 1$$

$$2^{qp} + 1 \neq 2^p + 1$$

$$\text{or } 2^p + 1 \mid 2^m + 1$$

$$2^m + 1 \neq 2^p + 1$$

$$2^p + 1 = 1$$

$\Leftrightarrow 2^p = 0$ aucun $p \in \mathbb{N}$ satisfait cette condition

donc $2^p + 1 \neq 1$

Ainsi $(2^p + 1) \in \mathcal{D}(2^m + 1)$ et $(2^p + 1) \neq 1$ ✓

$2^m + 1$ ne serait pas premier absolu. ✓

Dans ce cas, cela signifie que
 $m = 1 \times \text{puissance de } 2$
donc m est une puissance de 2.

Cas $q=1$

$$2^m + 1 = 2^0 + 1 \text{ et } \sum_{i=0}^{1-1} (2^0)^i (-1)^{1-1-i} = 1$$

i e seuls $2^m + 1$ et 1 divisent $2^m + 1$

Conclusion $2^m + 1$ premier si $m = 2^k, k \in \mathbb{N}$

2. Puisque $m \in \mathbb{N}^* \mid m \geq 1$ et si $m = 2^n$

Ainsi 2^{2^n} est pair ✓

et $2^{2^n} + 1$ est impair ✓

$$3 (a) M_q F_{n+1} = (F_n - 1)^2 + 1$$

$$\bullet F_{n+1} = 2^{2^{n+1}} + 1 = 2^{2^n \times 2} + 1 \quad \checkmark$$

$$\begin{aligned} \bullet (F_n - 1)^2 + 1 &= (2^{2^n} + 1 - 1)^2 + 1 \\ &= (2^{2^n})^2 + 1 \\ &= 2^{2^n \times 2} + 1 \quad \checkmark \end{aligned}$$

$$\text{donc } F_{n+1} = (F_n - 1)^2 + 1 \quad \checkmark$$

$$3. b) \text{ Montrer } \prod_{k=0}^n F_k = F_{n+1} - 2$$

$$\forall n \in \mathbb{N}, \text{ soit } \mathcal{P}(n) : \left(\prod_{k=0}^n F_k = F_{n+1} - 2 \right)$$

Initialisation: Pour $n=0$

$$\prod_{k=0}^0 F_k = F_0 = 2^0 + 1 = 3 \quad \checkmark$$

$$F_1 - 2 = 2^1 + 1 - 2 = 5 - 2 = 3 \quad \checkmark \quad \left. \begin{array}{l} \prod_{k=0}^0 F_k = F_0 = 3 \\ F_1 - 2 = 3 \end{array} \right\} \mathcal{P}(0) \text{ vraie}$$

Hérédité: Soit $n \in \mathbb{N}$, on suppose $\mathcal{P}(n)$

$$\prod_{k=0}^{n+1} F_k = \left(\prod_{k=0}^n F_k \right) \times F_{n+1} \quad \checkmark$$

$$= (F_{n+1} - 2) \times F_{n+1} \quad \checkmark$$

$$= F_{n+1}^2 - 2F_{n+1} + 1 + 1 - 2 \quad \checkmark$$

$$= (F_{n+1} - 1)^2 + 1 \quad \text{d'après 3.a) } \left(\begin{array}{l} \text{c'est} \\ \text{correct} \end{array} \right)$$

$$= F_{n+2} - 2 \quad \checkmark$$

$\mathcal{P}(n+1)$ vraie. $\checkmark$

Conclusion: $\prod_{k=0}^n F_k = F_{n+1} - 2 \quad \checkmark$

4. Prenons $n < m$ (quitte à les intervertir)

$$\begin{aligned} \bar{F}_m &= (F_m - 2) + 2 \quad \text{D'après 3 (b)} \\ &= \prod_{k=0}^{m-1} F_k + 2 \\ &= F_n \times \underbrace{\prod_{\substack{k=0 \\ k \neq n}}^{m-1} F_k}_q + \underbrace{2}_r \end{aligned}$$

on a : $0 < 2 < F_n$ ✓
car $F_n = 2^{2^n} + 1 \geq 3$ ✓
 ≥ 2

Ainsi $F_m \wedge F_n = F_n \wedge 2$, or F_n est impair ×

Donc $F_m \wedge F_n = 1$ ✓

D'après
la question 2

T.B.