Nombres de Fermat, Mersenne et Fibonacci

blogdemaths.wordpress.com

1 Nombres de Fermat

On définit la suite (F_n) des nombres de Fermat par :

$$\forall n \in \mathbb{N}, F_n = 2^{2^n} + 1$$

Théorème — . *Pour tout $m > 0$,*

$$F_m = F_0 \times F_1 \times \ldots \times F_{m-1} + 2$$

Démonstration. Le théorème est évidemment vrai si $m = 1$.
Soit $m > 0$.

$$F_{m+1} - 2 = 2^{2^{m+1}} - 1 = (2^{2^m})^2 - 1 = (2^{2^m} - 1)(2^{2^m} + 1) = (F_m - 2)F_m$$

Donc, par récurrence, si on suppose que $F_m = F_0 \times F_1 \times \ldots \times F_{m-1} + 2$ alors

$$\begin{aligned} F_{m+1} &= (F_m - 2)F_m + 2 \\ &= (F_0 \times F_1 \times \ldots \times F_{m-1}) \times F_m + 2 \\ &= F_0 \times F_1 \times \ldots \times F_{m-1} \times F_m + 2 \end{aligned}$$

ce qui prouve le théorème. □

2 Nombres de Mersenne

On définit la suite (M_n) de nombres de Mersenne par :

$$\forall n \in \mathbb{N}, M_n = 2^n - 1$$

Théorème — . *Pour tout $m > n$,*

$$\mathrm{PGCD}(M_m, M_n) = M_{\mathrm{PGCD}(m,n)}$$

Autrement dit, $\mathrm{PGCD}(2^m - 1, 2^n - 1) = 2^{\mathrm{PGCD}(m,n)} - 1$.

Démonstration. Si $m > n$, alors on peut faire la division euclidienne de m par n :

$$m = nq + r \text{ avec } r < n$$

Ainsi,

$$\begin{aligned}
2^m - 1 &= 2^m - 2^{nq} + 2^{nq} - 1 \\
&= 2^{nq+r} - 2^{qn} + 2^{qn} - 1 \\
&= 2^{qn} \times 2^r - 2^{nq} + 2^{nq} - 1 \\
&= 2^{qn}(2^r - 1) + (2^n)^q - 1 \\
&= 2^{qn}(2^r - 1) + (2^n - 1)(1 + 2^n + 2^{2n} + \ldots + 2^{(q-1)n})
\end{aligned}$$

Donc,

$$\mathrm{M}_m = 2^{nq}\mathrm{M}_r + \mathrm{M}_n(1 + 2^n + 2^{2n} + \ldots + 2^{(q-1)n})$$

Montrons alors que les diviseurs communs à M_m et M_n sont identiques aux diviseurs communs à M_n et M_r.

- Si d est un diviseur commun à M_m et M_n alors d divise $\mathrm{M}_m - \mathrm{M}_n(1 + 2^n + 2^{2n} + \ldots + 2^{(q-1)n}) = 2^{nq}\mathrm{M}_r$. Mais comme d divise le nombre M_n qui est impair, d ne peut diviser 2 et donc nécessairement, d divise M_r.

- Réciproquement, si d divise M_n et M_r alors d divise $2^{nq}\mathrm{M}_r + \mathrm{M}_n(1 + 2^n + 2^{2n} + \ldots + 2^{(q-1)n}) = \mathrm{M}_m$. Nous avons donc montré que les diviseurs communs de M_m et M_n sont les mêmes que les diviseurs communs de M_n et M_r. D'où :

$$\mathrm{PGCD}(\mathrm{M}_m, \mathrm{M}_n) = \mathrm{PGCD}(\mathrm{M}_n, \mathrm{M}_r)$$

Si on considère la suite (r_n) des restes successifs dans l'algorithme d'Euclide appliqué à m et n, et si on note r_N le dernier reste non nul (qui se trouve être le PGCD de m et n) alors :

$$\begin{cases}
\mathrm{PGCD}(\mathrm{M}_m, \mathrm{M}_n) & = \mathrm{PGCD}(\mathrm{M}_n, \mathrm{M}_{r_0}) \\
\mathrm{PGCD}(\mathrm{M}_n, \mathrm{M}_{r_0}) & = \mathrm{PGCD}(\mathrm{M}_{r_0}, \mathrm{M}_{r_1}) \\
\ldots & \\
\mathrm{PGCD}(\mathrm{M}_{r_{\mathrm{N}-1}}, \mathrm{M}_{r_\mathrm{N}}) & = \mathrm{PGCD}(\mathrm{M}_{r_\mathrm{N}}, \mathrm{M}_0)
\end{cases}$$

Or, $\mathrm{M}_0 = 0$ donc $\mathrm{PGCD}(\mathrm{M}_m, \mathrm{M}_n) = \mathrm{PGCD}(\mathrm{M}_{r_\mathrm{N}}, \mathrm{M}_0) = \mathrm{M}_{r_\mathrm{N}} = \mathrm{M}_{\mathrm{PGCD}(m,n)}$. CQFD. □

3 Nombres de Fibonacci

On définit la suite (f_n) des nombres de Fibonacci par :

$$\begin{cases}
f_0 & = 0 \\
f_1 & = 1 \\
f_{n+2} & = f_{n+1} + f_n \text{ pour tout } n \in \mathbb{N}
\end{cases}$$

Théorème — . *Pour tout $m > n$,*

$$\mathrm{PGCD}(f_m, f_n) = f_{\mathrm{PGCD}(m,n)}$$

Démonstration. Le principe est similaire à celui mis en oeuvre pour les nombres de Mersenne.

Etape 1 :

On commence par montrer l'égalité suivante :

$$\forall u, v > 0, f_{u+v} = f_u f_{v+1} + f_{u-1} f_v \tag{1}$$

On fixe v et on fait une récurrence sur u.

- Si $u = 1$, $f_u f_{v+1} + f_{u-1} f_v = 1 \times f_{v+1} + 0 \times f_v = f_{1+v}$
- On suppose l propriété vraie au rang u.

$$\begin{aligned} f_{u+1+v} &= f_{u+(v+1)} \\ &= f_u f_{v+2} + f_{u-1} f_{v+1} \\ &= f_u (f_{v+1} + f_v) + f_{u-1} f_{v+1} \\ &= (f_u + f_{u-1}) f_{v+1} + f_u f_v \\ &= f_{u+1} f_{v+1} + f_u f_v \end{aligned}$$

CQFD.

Etape 2 :

On montre par récurrence que pour tout entier $v > 0$ et tout entier naturel q, f_v divise f_{qv} (la récurrence est faite sur q) :

- Si $q = 0$, le résultat est évident car f_v divise $f_0 = 0$.
- On suppose que f_v divise f_{qv}. D'après l'égalité (1), on a :

$$\begin{aligned} f_{(q+1)v} &= f_{qv+v} \\ &= f_{qv} f_{v+1} + f_{qv-1} f_v \end{aligned}$$

et comme f_v divise f_{qv} et f_v, il divise $f_{qv} f_{v+1} + f_{qv-1} f_v$ donc $f_{(q+1)v}$.

Etape 3 :

On montre que deux nombres de Fibonacci consécutifs sont premiers entre eux, c'est-à-dire que pour tout entier naturel n, $\mathrm{PGCD}(f_n, f_{n+1}) = 1$.

- C'est vrai si $n = 0$ car $\mathrm{PGCD}(f_0, f_1) = \mathrm{PGCD}(0, 1) = 1$.
- On suppose que $\mathrm{PGCD}(f_n, f_{n+1}) = 1$.
  Si d est un diviseur commun à f_{n+1} et f_{n+2} alors d divise $f_{n+2} - f_{n+1} = f_n$. Ainsi, d est un diviseur commun à f_{n+1} et f_n donc $d = 1$ (car par hypothèse de récurrence, le plus grand diviseur commun à f_{n+1} et f_n est 1).

Etape 4 :

A présent, passons à la démonstration du théorème à proprement parler.
Soit $m > n$. On commence par effectuer la division euclidienne de m par n :

$$m = nq + r \text{ avec } r < n$$

En appliquant l'égalité (1) démontrée précédemment à $u = nq$ et $v =$r, on obtient :

$$\begin{aligned} f_m &= f_{nq+r} \\ &= f_{nq} f_{r+1} + f_{nq-1} f_r \end{aligned}$$

Comme pour les nombres de Mersenne, on montre que les diviseurs commun à f_m et f_n sont identiques aux diviseurs commun à f_n et f_r :

- Si d divise f_m et f_n alors il divise f_m et f_{nq} (voir étape 2) donc il divise $f_m - f_{nq}f_{r+1} = f_{nq-1}f_r$. Mais comme f_{nq} et f_{nq-1} sont consécutifs, ils sont premiers entre eux (étape 3), donc, puisque d divise f_{nq}, il est lui aussi premier f_{nq-1}. Mais puisque d divise le produit $f_{nq-1}f_r$, c'est qu'il divise f_r.
- Réciproquement, si d divise f_n et f_r, alors d divise f_{nq} (étape 2) et donc il divise $f_{nq}f_{r+1} + f_{nq-1}f_r = f_m$.

On en déduit que $\mathrm{PGCD}(f_m, f_n) = \mathrm{PGCD}(f_n, f_r)$ et le même raisonnement utilisant l'algorithme d'Euclide que celui effectué pour les nombres de Mersenne montre que :

$$\mathrm{PGCD}(f_m, f_n) = \mathrm{PGCD}(f_{r_N}, f_0) = \mathrm{PGCD}(f_{\mathrm{PGCD}(m,n)}, 0) = f_{\mathrm{PGCD}(m,n)}$$

□