TD 10

Divisibilité, PGCD, PPCM

6. (a) On raisonne par récurrence.

Initialisation On a $F_0\ F_2 - F_1^2 = -1 = (-1)^1$ donc la formule est vraie au rang 1.
Hérédité Supposons que $F_{n-1}\ F_{n+1} - F_n^2 = (-1)^n$ pour un certain $n \in \mathbb{N}^*$.

$$\begin{aligned} F_n\ F_{n+2} - F_{n+1}^2 &= F_n\,(\ F_{n+1} + F_n) - F_{n+1}\,(\ F_{n-1} + F_n) \\ &= F_n^2 - F_{n+1}\ F_{n-1} = -(-1)^n = (-1)^{n+1} \end{aligned}$$

La formule est donc également vraie au rang $n+1$.
Conclusion La formule est vraie pour tout $n \in \mathbb{N}^*$.
On a donc une relation de Bézout entre F_n et F_{n-1} : ces deux entiers sont donc premiers entre eux.

(b) On raisonne par récurrence sur n (et pas sur p). L'hypothèse de récurrence au rang $n \in \mathbb{N}$ est la suivante : (H_n) : Pour tout $p \in \mathbb{N}^*,\ F_{n+p} = F_p\ F_{n+1} + F_{p-1}\ F_n$.
Initialisation On a pour tout $p \in \mathbb{N}^*$:

$$F_p\ F_1 + F_{p-1}\ F_0 = F_p$$

donc (H_0) est vraie.
Hérédité Supposons (H_n) pour un certain $n \in \mathbb{N}$. Soit $p \in \mathbb{N}^*$. Remarquons que $F_{(n+1)+p} = F_{n+(p+1)}$. Or $p+1 \in \mathbb{N}^*$. On applique notre hypothèse de récurrence (H_n) :

$$\begin{aligned} F_{n+(p+1)} &= F_{p+1}\ F_{n+1} + F_p\ F_n \\ &= (F_p + F_{p-1})\, F_{n+1} + F_p\ F_n \\ &= F_p\,(\ F_{n+1} + F_n) + F_{p-1}\ F_{n+1} \\ &= F_p\ F_{n+2} + F_{p-1}\ F_{n+1} \end{aligned}$$

Ceci étant vrai quelque soit le choix de p, on en déduit que (H_{n+1}) est vraie.
Conclusion Pour tout $n \in \mathbb{N}, (\mathrm{H}_n)$ est vraie.
Soit $(n,p) \in \mathbb{N} \times \mathbb{N}^*$.

— Soit d un diviseur comun de F_n et F_p. Comme $\mathrm{F}_{n+p} = \mathrm{F}_p\ \mathrm{F}_{n+1} + \mathrm{F}_{p-1}\ \mathrm{F}_n, d$ divise également F_{n+p}. Donc d est un diviseur commun de F_p et F_{n+p}.

— Réciproquement, soit d un diviseur commun de F_p et F_{n+p}. On en déduit que d divise $\mathrm{F}_{p-1}\ \mathrm{F}_n$ Or F_p et F_{p-1} sont premiers entre eux et d divise F_p, donc d et F_{p-1} sont également premiers entre eux. D'après le théorème de Gauss, d divise F_n. C'est donc un diviseur commun de F_n et F_p.
  On en conclut que $\mathrm{F}_n \wedge\ \mathrm{F}_p = \mathrm{F}_{n+p} \wedge\ \mathrm{F}_p$.

(c) Soit $(m,n) \in \mathbb{N}^2$. On effectue la division euclidienne de m par n : $m = nq + r$. En itérant le résultat de la question précédente, on a

$$\mathrm{F}_n \wedge\ \mathrm{F}_r = \mathrm{F}_n \wedge\ \mathrm{F}_{r+n} = \mathrm{F}_n \wedge\ \mathrm{F}_{r+2n} = \cdots = \mathrm{F}_n \wedge\ \mathrm{F}_{r+nq} = \mathrm{F}_n \wedge\ \mathrm{F}_m$$

On conclut grâce à l'algorithme d'Euclide. Soit $d = m \wedge n$. Notons $a_0, \ldots, a_m = d$ la suite des restes non nuls obtenus par l'algorithme d'Euclide. D'après ce qui précéde,

$$\mathrm{F}_m \wedge\ \mathrm{F}_n = \mathrm{F}_n \wedge\ \mathrm{F}_{a_0} = \mathrm{F}_{a_0} \wedge\ \mathrm{F}_{a_1} = \cdots = \mathrm{F}_{a_m} \wedge\ \mathrm{F}_0 = \mathrm{F}_d$$

8. Raisonnons par récurrence sur n.
   La propriété est évidente au rang $n = 0$. Supposons-la vraie à un certain rang $n \in \mathbb{N}$. Remarquons que

$$5^{2^{n+1}} - 1 = \left(5^{2^n}\right)^2 - 1 = \left(5^{2^n} - 1\right)\left(5^{2^n} + 1\right)$$

D'après l'hypothèse de récurrence 2^{n+2} est la plus grand puissance de 2 divisant $5^{2^n} - 1$. Montrons que 2 est la plus grande puissance de 2 divisant $5^{2^n} + 1$. On sait que $5 \equiv 1$ [4]. Donc $5^{2^n} + 1 \equiv 2$ [4]. Ceci prouve que 2 divise $5^{2^n} + 1$ mais que 4 ne le divise pas.
En conclusion, 2^{n+3} est la plus grande puissance de 2 divisant $5^{2^{n+1}} - 1$.

Entiers premiers entre eux

16. Remarquons qu'aucun des entiers x, y, z ne peut être égal à 1 . De plus, on ne peut avoir $x > 3, y > 3$ et $z > 3$ car sinon $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < 1$.

Donc l'un des trois entiers est inférieur ou égal à 3 . Supposons que ce soit x : on peut avoir $x=2$ ou $x=3$.
Cas $x=2$: On a alors $\frac{1}{y}+\frac{1}{z}=\frac{1}{2}$. Comme auparavant, aucun des entiers y et z ne peut être égal à 2 et on ne peut avoir $y>4$ et $z>4$. L'un de ces deux entiers est donc inférieur ou égal à 4 . Supposons que ce soit y.

Cas $y=3$: On obtient $z=6$.
Cas $y=4$: On obtient $z=4$.
Cas $x=3$: On a alors $\frac{1}{y}+\frac{1}{z}=\frac{2}{3}$. On ne peut avoir $y>3$ et $z>3$. L'un de ces deux entiers est donc inférieur ou égal à 3 . Supposons que ce soit y.
Cas $y=2$: On obtient $z=6$.
Cas $y=3$: On obtient $z=3$.
En conclusion, les solutions sont les triplets $(2,3,6),(2,4,4),(3,3,3)$ et toutes les permutations de ceux-ci.

Approfondissements

19. Posons $\mathrm{A}=10^{10^n}$. On a $\mathrm{A}\equiv 3^{10^n}[7]$ et, puisque 7 est un nombre premier ne divisant pas 3 , d'après le petit théorème de Fermat, $3^6\equiv 1[7]$. Recherchons donc le reste de 10^n modulo 6 , c'est-à-dire le reste de 4^n modulo 6 . On obtient $4^2\equiv 4[7]$, puis, pour tout entier $n\geq 2$,

$$4^n\equiv 4^2 4^{n-2}\equiv 4\cdot 4^{n-2}\equiv 4^{n-1}[6]$$

On a donc, pour $n\geq 1,4^n\equiv 4[6]$ et $A\equiv 3^4=81\equiv 4[7]$.

20. (a) On a $\lfloor nx\rfloor\leq nx$ puis $\frac{\lfloor nx\rfloor}{n}\leq x$, or $x\mapsto\lfloor x\rfloor$ est croissante donc

$$\left\lfloor\frac{\lfloor nx\rfloor}{n}\right\rfloor\leq\lfloor x\rfloor$$

$\lfloor x\rfloor\leq x$ donc $n\lfloor x\rfloor\leq nx$ puis $n\lfloor x\rfloor\leq\lfloor nx\rfloor$ car $n\lfloor x\rfloor\in\mathbb{Z}$.
Par suite

$$\lfloor x\rfloor\leq\frac{\lfloor nx\rfloor}{n}$$

puis

$$\lfloor x\rfloor\leq\left\lfloor\frac{\lfloor nx\rfloor}{n}\right\rfloor$$

et finalement

$$\lfloor x \rfloor = \left\lfloor \frac{\lfloor nx \rfloor}{n} \right\rfloor$$

(b) En isolant les multiples de p dans le produit décrivant $p\,!$, on obtient

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + v_p\left(\left\lfloor \frac{n}{p} \right\rfloor !\right)$$

puis

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor + v_p\left(\left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor !\right)$$

or

$$\left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$$

avec $x = n/p^2$ donne

$$\left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor$$

puis finalement

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor$$

avec

$$k = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor.$$

21. L'ensemble de l'énoncé est formé des entiers de la forme $u_n = \sum\limits_{k=0}^{n} 10^k$ pour $n \in \mathbb{N}$. On a facilement $u_n = \frac{1}{9}\left(10^{n+1} - 1\right)$. Soit p un entier premier différent de 2 , 3 et 5 . Alors $10 = 2 \times 5$ est premier avec p. D'après le petit théorème de Fermat, $10^{p-1} \equiv 1[p]$ donc p divise $10^{p-1} - 1$. Comme $p \neq 3$, p est premier avec 9 . On sait que 9 divise $10^{p-1} - 1$ puisque $\frac{1}{9}\left(10^{p-1} - 1\right) = u_{p-2} \in \mathbb{N}$. Donc $9p$ divise $10^{p-1} - 1$ i.e. p divise u_{p-2}.

22. Soient p et q deux nombres premiers consécutifs avec $p < q$.
Si $p = 2$, alors $q = 3$ et $p + q = 5$ ne peut être le produit de deux nombres premiers.
Si $p > 2$, alors p et q sont impairs donc $p + q$ est pair. Supposons qu'il existe deux nombres premiers a et b tels que $p + q = ab$. Comme $p + q$ est pair, un des deux nombres premiers a et b est égal à 2 par unicité de la décomposition en facteurs premiers. Supposons sans perte de généralité que $a = 2$. Alors $b = \frac{p+q}{2}$ est un nombre premier strictement compris entre p et q, ce qui contredit le fait que p et q sont des nombres premiers consécutifs.