121. Nombres premiers : solutions

1. a) Soit $m > 1$ un entier avec $m \leq n$. Alors m divise $n!$, donc il ne peut pas diviser $(n!)^2 + 1$. Ainsi $p > n$.

b) On a $(n!)^2 + 1$ congru à 0 modulo p, donc -1 est un carré modulo p, et on sait qu'alors p est congru à -1 modulo 4 (ou alors $p = 2$, ce qui ne peut se produire que pour $n = 1$ sinon $(n!)^2 + 1$ est impair).

c) Si $\varepsilon = 1$, a) et b) montrent que pour tout $n > 1$, il existe un nombre premier p congru à 1 modulo 4 avec $p > n$, ce qui donne le résultat.

Si maintenant $\varepsilon = -1$, supposons par l'absurde qu'il y ait un nombre fini (non vide vu que 3 en fait partie) de nombres premiers congru à -1 modulo 4, soit $p_1, ..., p_r$. Soit $N = 4p_1...p_r - 1$. Alors comme $2, p_1, ..., p - r$ ne divisent pas N, tous les diviseurs premiers de N seraient congrus à 1 modulo 4, donc aussi leur produit N (noter que $N > 1$). Or N est congru à 1 modulo 4, contradiction.

2. Rappelons que $\mathbf{Z}[i]$ est principal et que ses inversibles sont ± 1 et $\pm i$.

a) Si $p = a^2 + b^2$, alors $p = (a + ib)(a + ib)$ n'est pas irréductible (noter qu'on ne peut avoir $a = 0$ ou $b = 0$, donc aucun des deux facteurs n'est inversible). Réciproquement, si p n'est pas irréductible, il s'écrit $p = xy$ avec x, y dans A non inversibles. En particulier $N(x) := \bar{x}x$ et $N(y)$ sont des entiers naturels ≥ 2 et on a $N(p) = p^2 = N(x)N(y)$. La seule possibilité est alors $N(x) = N(y) = p$, d'où $p = \bar{x}x$ est de la forme $a^2 + b^2$ en posant $x = a + ib$ avec $a, b \in \mathbf{Z}$.

b) Si $p \in \mathbf{N}^*$ est irréductible dans A, on a déjà que p est premier, sinon $p = uv$ avec u, v au moins égaux à 2 (en particulier u et v sont non inversibles dans A). Réciproquement, un tel p est irréductible si et seulement s'il est somme de deux carrés d'après a), i.e. s'il est congru à 1 modulo 4. Il en va de même de $-p$ et $\pm ip$ qui lui sont associés.

On s'intéresse maintenant aux $z = a + ib$ avec a, b non nuls dans $\mathbf{Z}$. On note que si $N(z) = a^2 + b^2$ est premier, alors z est irréductible : si $z = z_1 z_2$ avec z_1, z_2 dans A, on a $N(z) = N(z_1)N(z_2)$, ce qui implique que $N(z_1)$ ou $N(z_2)$ vaut 1 et donc que z_1 ou z_2 est inversible.

Supposons réciproquement que z est irréductible Soit p un diviseur premier de $N(z)$ (qui est > 1). Si p est congru à -1 modulo 4, il est irréductible dans A, donc il divise z ou $\bar{z}$ dans l'anneau principal A, vu qu'il divise leur produit. Si p divise $\bar{z}$, il divise aussi z (en conjuguant), donc lui est associé ce qui est impossible. Les seuls diviseurs premiers de $N(z)$ sont donc congrus à 1 modulo 4, ou encore de la forme $p = c^2 + d^2$ avec c, d dans $\mathbf{N}^*$. Alors p est divisible par $c + id$ qui est irréductible (d'après ce qu'on a vu plus haut) et divise z ou $\bar{z}$ (car il divise $z\bar{z}$), ce qui implique que $c + id$ est associé à z ou $\bar{z}$, et finalement que $N(z) = c^2 + d^2 = p$ est premier.

Finalement les irréductibles de $\mathbf{Z}[i]$ sont les nombres premiers p congrus à -1 modulo 4 (et leurs associés), ainsi que les $a + ib$ avec a, b entiers non nuls avec $a^2 + b^2$ premier.

c) On a ici a et b non nuls. Alors on n'a pas $z = \pm\bar{z}$. D'autre part $iz = ia - b$ est égal à $\pm\bar{z}$ si et seulement si $a = b$ ou $a = -b$, donc le seul cas où z et $\bar{z}$ sont associés sont quand ils sont égaux à $1 + i$ et $1 - i$, sinon $N(z) = 2a^2$ n'est pas un nombre premier.

3. a) On a $p^2 - 1 = (p - 1)(p + 1)$ avec $p - 1$ et $p + 1$ pairs et l'un deux divisible par 4, donc $p^2 - 1$ est divisible par 8.

b) Soit a un générateur du groupe cyclique $\mathbf{F}_{p^2}^*$, alors a est d'ordre $p^2 - 1$. Posons $k = (p^2 - 1)/8$, c'est un entier d'après a) et $b = a^k$ est d'ordre 8, ce qui signifie que $b^4 = -1$ donc b est racine de Q.

c) Si Q était un polynôme irréductible, une racine α de Q (dans un corps de décomposition de Q sur $\mathbf{F}_p$) vérifierait $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = 4]$, ce qui contredit b). Si $p = 2$, alors $Q = (X + 1)^4$ et le résultat vaut donc encore.

d) On sait que dans $\mathbf{Z}[X]$, on a pour tout $m > 0$:

$$X^m - 1 = \prod_{n|m} \Phi_n(X).$$

Le résultat en découle facilement par récurrence sur n.

e) Supposons que l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$ est $m < \varphi(n)$. Alors n divise $p^m - 1$, et comme $\mathbf{F}_{p^m}$ est cyclique, il contient un élément b d'ordre exactement n, i.e. b est une racine primitive n-ième de l'unité dans $\mathbf{F}_{p^m}$. Ceci implique d'après d) que $\Phi_{n,p}(b) = 0$, et donc $\Phi_{n,p}$ (qui est de degré $\varphi(n)$) ne peut pas être irréductible sur $\mathbf{F}_p$ vu qu'il a une racine dans une extension de $\mathbf{F}_p$ de degré $m < \varphi(n)$.

En sens inverse, si p est d'ordre $\varphi(n)$ dans $(\mathbf{Z}/n\mathbf{Z})^*$, alors pour tout $m < \varphi(n)$, le corps $\mathbf{F}_{p^m}$ ne contient pas de racine n-ième de l'unité (sinon n diviserait $p^m - 1$ via le théorème de Lagrange), donc toute racine de $\Phi_{n,p}$

(dans un corps de décomposition sur $\mathbf{F}_p$) est de degré $>= \varphi(n)$ sur $\mathbf{F}_p$, ce qui implique que $\Phi_{n,p}$ est irréductible sur $\mathbf{F}_p$ (sinon il aurait un facteur irréductible de degré $d < \varphi(n)$, lequel aurait une racine dans une extension de $\mathbf{F}_p$ de degré d).

4. On décompose n en facteurs premiers :

$$n = 2^\beta p_1^{\alpha_1} ... p_r^{\alpha_r},$$

où les p_i sont des nombres premiers impairs, $\beta \in \mathbf{N}$ et $\alpha_i \in \mathbf{N}^*$. Le lemme chinois dit alors que le groupe $G := (\mathbf{Z}/n\mathbf{Z})^*$ est isomorphe à

$$(\mathbf{Z}/2^\beta\mathbf{Z})^* \times (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^* \times ... \times (\mathbf{Z}/p_r^{\alpha_r}\mathbf{Z})^*.$$

On note que les $(\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^*$ sont des groupes cycliques d'ordre pair, chacun contient donc un groupe isomorphe au groupe additif $\mathbf{Z}/2\mathbf{Z}$. Ainsi, si G est cyclique, on a déjà $r \leq 1$, sinon G contiendrait un sous-groupe isomorphe au groupe additif $(\mathbf{Z}/2\mathbf{Z})^2$. D'autre part, le groupe $(\mathbf{Z}/2^\beta\mathbf{Z})^*$ est d'ordre pair, et de plus il n'est pas cyclique pour $\beta \geq 3$, donc dans ce dernier cas G n'est pas cyclique vu qu'il contient un sous-groupe isomorphe à $(\mathbf{Z}/2^\beta\mathbf{Z})^*$. Ainsi, G cyclique implique $\beta \leq 2$ et $r \leq 1$, mais par ailleurs si $r = 1$ et $\beta = 2$, le groupe G contient encore un sous-groupe isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$, et donc n'est pas cyclique. Les cas restants sont donc $n = 1$, $n = 2$, $n = 4$, $n = p^\alpha$ avec p premier impair et $\alpha \geq 1$, et $n = 2p^\alpha$ avec p premier impair et $\alpha \geq 1$. Ces cas conviennent bien via le lemme chinois, vu qu'on sait que $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique.

5. a) Supposons $n > 1$ non premier (pour $n = 1$, on a bien que $2^n - 1 = 1$ n'est pas premier). Alors $n = rs$ avec r, s entiers ≥ 2. De plus, $2^n - 1 = (2^r)^s - 1$ est divisible par $d := 2^r - 1$: en effet 2^r est congru à 1 modulo d. Ainsi $2^n - 1$ n'est pas premier vu que $1 < 2^r - 1 < 2^n - 1$.

b) Si n n'est pas une puissance de 2, on peut écrire $n = ab$ avec $b \in \mathbf{N}^*$ et $a \geq 3$ impair. Posons $d = 2^b + 1$, alors $2^b \equiv -1 \pmod{d}$, d'où $(2^b)^a \equiv -1 \pmod{d}$ puisque a est impair. Ainsi d divise $2^n + 1$, qui n'est donc pas premier vu que $1 < d < 2^n + 1$.

6. La série est de la même nature que $\sum -\log(1 - 1/p_n)$ (par équivalence du terme général des deux séries, qui sont à termes positifs), et donc que le produit infini $\prod \frac{1}{1-1/p_n}$. Le terme général de ce produit est $u_n := \sum_{k=0}^{+\infty} \frac{1}{p_n^k}$. Soit $A > 0$, comme la série $\sum 1/n$ est divergente, il existe $M > 0$ tel que $\sum_{m=1}^{M} 1/m \geq A$. Soit alors K et N des entiers tels que tous les entiers de 1

à M s'écrivent sous la forme $p_1^{k_1}...p_r^{k_r}$ avec $r \leq N$ et tous les k_i égaux au plus à K. Alors

$$\prod_{n=1}^{N} u_n \geq \prod_{n=1}^{N} \sum_{k=0}^{K} \frac{1}{p_n^k} \geq \sum_{m=1}^{M} 1/m \geq A$$

via l'existence et l'unicité de la décomposition en facteurs premiers de tout entier entre 1 et M. Ainsi $\prod u_n$ diverge vers $+\infty$, comme on voulait.

7. a) C'est vrai : en effet H est alors l'unique p-Sylow de G (car on sait que deux p-Sylow quelconques sont conjugués), or tout automorphisme de G envoie clairement un p-Sylow de G sur un p-Sylow de G.

b) C'est faux, prendre par exemple $G = \mathcal{S}_3$, qui n'est pas isomorphe à $\mathbf{Z}/2 \times \mathbf{Z}/3$ (alors qu'un 2-Sylow de G est isomorphe à $\mathbf{Z}/2$ et un 3-Sylow à $\mathbf{Z}/3$). Le résultat est vrai pour un groupe abélien (via le théorème de structure), et en fait (plus difficile) il caractérise les groupes finis nilpotents.

c) C'est vrai. Soit A_p le *sous-groupe de torsion p-primaire* de A, défini par l'ensemble des éléments x tels qu'il existe $m \geq 0$ avec $p^m x = 0$. Définissons alors

$$\Phi : \bigoplus_{p \in \mathcal{P}} A_p \to A, (x_p)_{p \in \mathcal{P}} \mapsto \sum_{p \in \mathcal{P}} x_p$$

(rappelons que par définition de la somme directe, la famille (x_p) est presque nulle). On va montrer que Φ est un isomorphisme. Il s'agit en fait d'une version générale du lemme chinois.

i) Le noyau de Φ est trivial : si $x_1 + ... + x_r = 0$ avec $x_1, ..., x_r$ d'ordres respectifs $p_1^{m_1}, ..., p_r^{m_r}$ (où $p_1, ..., p_r$ sont des nombres premiers deux à deux distincts), alors $(p_2^{m_2}...p_r^{m_r})x_1 = 0$, donc par définition de l'ordre $p_2^{m_2}...p_r^{m_r}$ est divisible par $p_1^{m_1}$, ce qui implique $m_1 = 0$, puis $x_1 = 0$. On montre de même que $x_2, ..., x_r$ sont nuls.

ii) Soit $x \in A$, par hypothèse on a un entier $n > 0$ (qu'on peut supposer au moins égal à 2) tel que $nx = 0$. Décomposons n en facteurs premiers :

$$n = p_1^{m_1}...p_r^{m_r},$$

et montrons maintenant par récurrence sur r que x peut s'écrire comme une somme $x = \sum_{i=1}^{r} x_i$, où chaque x_i est dans A_{p_i}. Pour $r = 1$, on a déjà $x \in A_{p_1}$. Supposons le résultat vrai pour $r - 1$. D'après Bezout, on peut trouver $u, v \in \mathbf{Z}$ tels que

$$up_1^{m_1} + vp_2^{r_2}...p_r^{m_r} = 1$$

, d'où

$$x = up_1^{m_1}x + vp_2^{r_2}...p_r^{m_r}x.$$

On observe alors que $vp_2^{r_2}...p_r^{m_r}x \in A_{p_1}$ (il est annulé par multiplication par $p_1^{m_1}$) et on peut appliquer l'hypothèse de récurrence à $up_1^{m_1}$, qui est annulé par multiplication par $p_2^{r_2}...p_r^{m_r}$. Le résultat en découle.