Exercice 6 (Théorème d'Euler)
Le théorème que l'on devine est :

$$\sum_{\substack{0\leq i\leq n-1\\(i,n)=1}} i = \frac{n}{2}\varphi(n)$$

pour tout $n \geq 3$. Pour le montrer, on remarque d'abord que si $(i,n) = 1$, alors $(n-i,n) = 1$. En effet, si $(i,n) = 1$ et d est un diviseur commun de $n-i$ et n, alors d divise aussi $i = n-(n-i)$ est donc $d = 1$ ou $d = -1$. On en déduit que

$$\{i \in \mathbb{Z} \mid 0 \leq i \leq n-1, (n,i) = 1\} = \{n-i \in \mathbb{Z} \mid 0 \leq i \leq n-1, (n,i) = 1\}.$$

Ainsi

$$\begin{aligned} 2\sum_{\substack{0\leq i\leq n-1\\(n,i)=1}} i &= \sum_{\substack{0\leq i\leq n-1\\(n,i)=1}} i + \sum_{\substack{0\leq i\leq n-1\\(n,i)=1}} n-i \\ &= \sum_{\substack{0\leq i\leq n-1\\(n,i)=1}} n \\ &= n\varphi(n) \end{aligned}$$

car $\varphi(n)$ est le nombre de $i \in \{0,\ldots,n-1\}$ tel que $(n,i) = 1$. On a donc prouvé notre théorème.

Exercice 6.2 (Logarithme discret)
On cherche les solutions de la congruence $x^4 \equiv 1 \bmod 17$. Donc on cherche les $x \in \mathbb{Z}$ tels que l'ordre de x modulo 17 soit un diviseur de 4. Les solutions sont donc les éléments d'ordre 1, 2 ou 4 modulo 17. Commençons par regarder les puissances de 2 modulo 17. On a

i	1	2	3	4
2^i	2	4	8	-1

Donc l'ordre de 2 modulo 17 est égal à 8. Cela suffit pour déduire les éléments d'ordre 2 et 4. On remarque que $4 = 2^2$ est d'ordre 4 modulo 17 et $-1 = 2^4$ est d'ordre 2 modulo 17.

Si a est d'ordre d modulo 17, pour trouver tous les éléments d'ordre d modulo 17, il faut prendre les a^i pour tout $i \in \{0,\ldots,d-1\}$ tels que $(d,i) = 1$. Donc -1 est le seul élément d'ordre 2 modulo 17 et, 4 et $4^3 = 2^4 \cdot 2^2 = -4$ sont les éléments d'ordre 4 modulo 17.

Donc les solutions de $x^4 \equiv 1 \bmod 17$ sont 1 (d'ordre 1), -1 (d'ordre 2) et, 4 et -4 (d'ordre 4).

Exercice 4 (Théorie analytique des nombres)
On ne montre que la 1ère partie de l'exercice, c'est-à-dire on montre que

$$\zeta(s)^{-1} = \prod_{p\in P}\Big(1-p^{-s}\Big) = \sum_{n\geq 1}\frac{\mu(n)}{n^s}$$

pour tout $s>1$, où μ est la fonction de Möbius et P est l'ensemble des nombres premiers. Par le théorème du produit, on a, pour tout $s>1$,

$$\zeta(s)^{-1} = \prod_{p\in P}\Big(1-p^{-s}\Big).$$

On va montrer la 2ème égalité. Soit $s>1$. Remarquons d'abord que la série $\sum_{n\geq 1}\frac{\mu(n)}{n^s}$ converge car elle converge absolument :

$$\sum_{n\geq 1}\Big|\frac{\mu(n)}{n^s}\Big| \leq \sum_{n\geq 1}\frac{1}{n^s} = \zeta(s).$$

On veut montrer que le produit $\prod_{p\in P}\left(1-p^{-s}\right)$ converge vers $\sum_{n\geq 1}\frac{\mu(n)}{n^s}$. Soit $N\in\mathbb{N}$ et soit $p_1,\dots,p_k$ tels que $P\cap[0,N]=\{p_1,\dots,p_k\}$. Alors

$$\prod_{p\in P\cap[0,N]}\Big(1-p^{-s}\Big) = \Big(1-\frac{1}{p_1^s}\Big)\Big(1-\frac{1}{p_2^s}\Big)\dots\Big(1-\frac{1}{p_k^s}\Big) = \sum_{\substack{n\geq 1\\ p\leq N, \forall p\in P \text{ avec } p/n}}\frac{\mu(n)}{n^s}.$$

Ainsi

$$\Big|\prod_{p\in P\cap[0,N]}\Big(1-p^{-s}\Big) - \sum_{n\geq 1}\frac{\mu(n)}{n^s}\Big| = \Big|\sum_{\substack{n\geq 1\\ \exists p\in P:\ p/n,\ p>N}}\frac{\mu(n)}{n^s}\Big|.$$

Or pour tout $M\in\mathbb{N}$,

$$\Big|\sum_{\substack{1\leq n\leq M\\ \exists p\in P:\ p/n,\ p>N}}\frac{\mu(n)}{n^s}\Big| \leq \sum_{\substack{1\leq n\leq M\\ \exists p\in P:\ p/n,\ p>N}}\Big|\frac{\mu(n)}{n^s}\Big| \leq \sum_{N\leq n\leq M}\frac{1}{n^s} \leq \sum_{n\geq N}\frac{1}{n^s},$$

donc

$$\Big|\sum_{\substack{n\geq 1\\ \exists p\in P:\ p/n,\ p>N}}\frac{\mu(n)}{n^s}\Big| \leq \sum_{n\geq N}\frac{1}{n^s}$$

Puisque la série $\zeta(s)$ converge, $\sum_{n\geq N}\frac{1}{n^s}$ tend vers 0 quand N tend vers l'infini. Donc

$$\Big|\prod_{p\in P\cap[0,N]}\Big(1-p^{-s}\Big) - \sum_{n\geq 1}\frac{\mu(n)}{n^s}\Big|$$

tend vers 0 quand N tend vers l'infini et

$$\prod_{p\in P}\Big(1-p^{-s}\Big) = \sum_{n\geq 1}\frac{\mu(n)}{n^s}.$$