Exercice 1 Pour tous $a, b \in \mathbf{Z}$, démontrer que $ab(a^{60} - b^{60})$ est multiple de 56786730.

Exercice 2 1) Soient p un nombre premier et $r \geq 1$. Montrer que les seuls idempotents de $\mathbf{Z}/p^r\mathbf{Z}$ sont $\dot{0}$ et $\dot{1}$.
2) En quoi peut-on en déduire que le lemme chinois est "optimal" ?
3) Relier la première question à la propriété d'être un anneau local.

Exercice 3 1) Soit p un nombre premier impair. Démontrer que, pour tout $k \geq 0$, on a $(1+p)^{p^k} = 1 + p^{k+1}x$ avec x entier non multiple de p.
2) En déduire que l'élément $1 + p \pmod{p^m}$ du groupe $(\mathbf{Z}/p^m\mathbf{Z})^*$ est d'ordre p^{m-1}.

Exercice 4 Soit $m \in \mathbf{N}^*$ et soit $d \in \mathbf{N}^*$ un diviseur de m. Dénombrer les entiers a de $\{1, \ldots, m\}$ tels que $a \wedge m = d$ et en déduire la formule :

$$\sum_{d|m} \phi(d) = m.$$

Exercice 5 1) Soit p premier. Montrer que pour tout diviseur d de $p-1$, il y a, dans le groupe $(\mathbf{Z}/p\mathbf{Z})^*$, au plus d éléments dont l'ordre divise d.
2) A l'aide de l'exercice précédent, en déduire que $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.
3) Démontrer de même que, si K est un corps commutatif, tout sous-groupe fini de K^* est cyclique.

Exercice 6 1) Soit p premier. On note x un générateur du groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^*$ (voir l'exercice précédent). Soit $m \geq 1$, et soit $y \in \mathbf{Z}/p^m\mathbf{Z}$ un antécédent de x par le morphisme canonique $\mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. Montrer que $y \in (\mathbf{Z}/p^m\mathbf{Z})^*$ et que son ordre est de la forme $(p-1)q$. Quel est l'ordre de l'élément $z := y^q$?
2) On suppose p impair. Montrer que $(\mathbf{Z}/p^m\mathbf{Z})^*$ est cyclique.

Exercice 7 1) On note $\lfloor x \rfloor$ la partie entière du réel x. Montrer que le nombre de $a \in \{1, \ldots, m\}$ tels que $v_p(a) \geq r$ est égal à $\lfloor m/p^r \rfloor$. En déduire la formule :

$$v_p(m!) = \sum_{r \geq 1} \lfloor m/p^r \rfloor.$$

2) Utiliser cette formule pour démontrer que, si $0 \leq n \leq m$, alors $\dfrac{m!}{n!(m-n)!}$ est un entier.

Exercice 8 Calculer $v_p(a \wedge b)$ et $v_p(a \vee b)$ (on note $a \vee b$ le ppcm de a et b). En déduire une égalité remarquable au sujet de $(a \wedge b)(a \vee b)$.

Exercice 9 Pour tout $x \in \mathbf{Q}$, on pose :

$$|x|_p := p^{-v_p(x)}.$$

Montrer que $d_p(x,y) := |x-y|_p$ définit une distance *ultramétrique* sur $\mathbf{Q}$; autrement dit, l'inégalité du triangle est remplacée par l'inégalité plus forte :

$$d_p(x,z) \leq \max\big(d_p(x,y), d_p(y,z)\big).$$

Exercice 10 Dénombrer les solutions de $x^2 = 1$ dans $\mathbf{Z}/n\mathbf{Z}$. (Cette formule sert en cryptographie, *cf.* le théorème de Rabin dans le livre de Demazure.)