Université Rennes 1, Année 2013-2014
Master 1 Math., Algèbre générale de base

Feuille d'exercices 1, correction

Exercice 3 (3) Par définition, l'ordre de k est le plus petit entier $m \geq 1$ tel que $mk = 0$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire tel que n divise mk dans $\mathbb{Z}$.

Supposons d'abord k et n premiers entre eux. Alors, d'après le lemme de Gauss, le fait que n divise mk implique que n divise m. Le plus petit entier $m \geq 1$ qui vérifie ceci est $m = n$, donc l'ordre de k est n.

Dans le cas général, notons d le pgcd de k et n. On peut donc écrire $k = dk'$ et $n = dn'$ avec k' et n' premiers entre eux. Si n divise mk, alors en simplifiant par d (c'est possible car $d \neq 0$ et $\mathbb{Z}$ est intègre...), on trouve que n' divise mk'. D'après le cas précédent (ou en invoquant directement le lemme de Gauss), on obtient que n' divise m. Réciproquement, $m = n'$ convient car $n'k = n'dk' = nk'$ est multiple de n. Ceci montre que l'ordre de k est n', que l'on peut écrire aussi $n/\mathrm{pgcd}(k, n)$.