Université de Genève
Section de Mathématiques

Algèbre I
Session de printemps 2009
Série 6, corrigé partiel

Ex.5

(i) On a $1! = 1$ et $2! = 2$ or $1 \equiv -1_{[2]}$ et $2 \equiv -1_{[3]}$.

(ii) Si $xy \equiv 1_{[p]}$, c'est que y est l'inverse de x dans $\mathbb{Z}/p\mathbb{Z}$. Il s'agit donc de montrer que 1 et -1 sont les seuls éléments de $\mathbb{Z}/p\mathbb{Z}$ à être leur propre inverse. Or $x^2 \equiv 1_{[p]}$ est équivalent à $x^2 - 1 \equiv (x+1)(x-1) \equiv 0_{[p]}$ et comme $\mathbb{Z}/p\mathbb{Z}$ est intègre puisque p est premier, cela est encore équivalent à $x \equiv 1_{[p]}$ ou $x \equiv -1 \equiv p - 1_{[p]}$.

Réciproquement, il est clair que $1^2 \equiv (-1)^2 \equiv 1_{[p]}$.

(iii) D'après ce qui précède, tous les entiers entre 2 et $p-2$ [1] sont distincts de leur inverse dans $\mathbb{Z}/p\mathbb{Z}$. Comme ce dernier anneau est commutatif, les termes de $2.3.\cdots.(p-2)$ peuvent donc être rassemblés par paires dont le produit vaut 1. Au final, on obtient $2.3.\cdots.(p-2) \equiv 2.2^{-1}.\cdots.(p-2).(p-2)^{-1} \equiv 1.\cdots.1 \equiv 1_{[p]}$.

(iv) Enfin, on a $(p-1)! \equiv 1.2.\cdots.(p-2).(p-1) \equiv 1.1.(p-1)_{[p]}$ d'après la question précédente et donc $(p-1)! \equiv p - 1 \equiv -1_{[p]}$.

Ex.6

(a),(b) L'exercice 5 a déjà montré que si n est premier, alors $(n-1)! \equiv -1_{[n]}$. Supposons maintenant que n est composé et posons $1 < q < n$ un diviseur non trivial de n. Distinguons maintenant plusieurs cas selon la valeur de $n/q \in [\![2, n-1]\!]$:

- $n/q \neq q$**:** alors q et n/q apparaissent comme facteurs distincts dans $(n-1)!$. Ce dernier est donc un multiple de $q.n/q = n$, autrement dit $(n-1)! \equiv 0_{[n]}$;
- $n/q = q > 2$**:** alors $n = q^2 > 2q$. Les entiers q et $2q$ apparaissent donc comme facteurs distincts dans $(n-1)!$, qui est donc un multiple de $2q^2$, donc de q^2. On conclut de même que $(n-1)! \equiv 0_{[n]}$;
- $n/q = q = 2$**:** alors $n = 4$ et on a $3! \equiv 2_{[4]}$.

[1] c'est ici qu'il faut avoir supposé $p \geq 5$