L2 MTH1314 2014-2015

Correction de l'exercice n°2 du TD n°3

1. L'entier n est non premier donc par définition, il existe deux entiers x et y tels que $1 < x < n$, $1 < y < n$ et
$$n = xy.$$
Ainsi évidemment cela donne modulo n,
$$xy = 0\ [n].$$
De plus comme $1 < x < n$ et $1 < y < n$ on a également, $x \neq 0\ [n]$ et $y \neq 0\ [n]$.
De la même façon, comme $1 < x < n$ et $1 < y < n$, ils apparaissent tous les deux dans le produit $(n-1)! = (n-1) \times (n-2) \times ... \times 3 \times 2$. Mais attention deux cas disctincts se produisent.
Premier cas : $x \neq y$**.** Dans ce cas les deux éléments apparaissent bien séparément dans le produit, par exemple si $y < x$,
$$(n-1)! = (n-1) \times (n-2) \times ... \times x \times ... \times y \times ... \times 3 \times 2.$$
Et donc,
$$\begin{aligned}(n-1)! &= (n-1) \times (n-2) \times ... \times (x+1) \times (x-1) \times ... \times (y+1) \times (y-1) \times ... \times 3 \times 2 \times xy \\ &= (n-1) \times (n-2) \times ... \times (x+1) \times (x-1) \times ... \times (y+1) \times (y-1) \times ... \times 3 \times 2 \times n \\ &= 0\ [n].\end{aligned}$$
Second cas : $x = y$**.** De façon alors un peu plus subtile, $n = x^2$. Or on a supposé $n \geqslant 5$ donc le premier carré est 9 et donc nécessairement $x \geqslant 3 > 2$. Ainsi en multpipliant par x cette inégalité,
$$x^2 = n > 2x.$$
Cette fois on obtient que x et $2x$ sont distincts et entre 2 et $n-1$. D'où,
$$\begin{aligned}(n-1)! &= (n-1) \times (n-2) \times ... \times 2x \times ... \times x \times ... \times 3 \times 2 \\ &= (n-1) \times (n-2) \times ... \times (2x+1) \times (2x-1) \times ... \times (x+1) \times (x-1) \times ... \times 3 \times 2 \times 2xx \\ &= (n-1) \times (n-2) \times ... \times (x+1) \times (x-1) \times ... \times (y+1) \times (y-1) \times ... \times 3 \times 2 \times 2n \\ &= 0\ [n],\end{aligned}$$
et le résultat reste le même.

2. Soit $x \in \{2, \ldots, p-2\}$, puisque $x \neq 0\ [p]$ et que p est premier on sait bien sûr que x est alors inversible. Donc par définition, il existe $y \in \{0, \ldots, p-1\}$ tel que $xy = 1\ [p]$.
Or si $y = 0$ alors $xy = 0 \neq 1\ [n]$ donc nécessairement $y \neq 0$.
De même si $y = 1$, alors $xy = x = 1\ [p]$. Or $x \neq 1\ [p]$ donc nécessairement $y \neq 1$.
Enfin et toujours de la même façon, si $y = p-1$ alors $xy = x(p-1) = x(-1) = -x\ [p]$.
Donc $-x = 1\ [p]$ et $x = -1 = p-1\ [p]$. Or $x \neq p-1$ donc nécessairement $y \neq p-1$ et finalement
$$y \in \{2, \ldots, p-2\}.$$
Ainsi à chaque élément x dans $\{2, \ldots, p-2\}$ on associe son inverse (qui existe car comme on l'a vu $x \neq 0$ et p est premier) $y = x^{-1}$ qui se trouve aussi dans $\{2, \ldots, p-2\}$. Cet inverse est unique bien sûr et l'inverse de l'inverse c'est lui même, $y^{-1} = (x^{-1})^{-1} = x$. Ainsi si à x

on associe son inverse y, à y on va bien associer x et on va de cette façon vouloir rassembler tous les éléments en couple avec leur inverse (x, x^{-1}). Cependant dernière chose à vérifier pour pouvoir tous les ranger par deux, il faut vérifier auparavant que x ne peut pas être son propre inverse. C'est-à-dire montrons que $x^2 = 1\ [p]$ est impossible.
Par l'absurde, sinon,

$$\begin{aligned} x^2 - 1 &= 0\ [p] \\ (x-1)(x+1) &= 0\ [p] \end{aligned}$$

Or nous sommes dans le corps $\mathbb{Z}/p\mathbb{Z}$ car p est premier. Donc un produit de facteurs est nul si et seulement si un des facteurs au moins est nul. Donc

$$x - 1 = 0\ [p] \qquad \text{ou} \qquad x + 1 = 0\ [p].$$

Donc,

$$x = 1\ [p] \qquad \text{ou} \qquad x = -1 = p - 1\ [p].$$

Ce qui est impossible car $x \in \{2, \ldots, p-2\}$. Donc on sait que $y \neq x$. Ainsi tous les éléments $\{2, \ldots, p-2\}$ peuvent être mis en couple, on peut tous les rassembler deux par deux et personne n'est laissé de côté. Ainsi

$$(p-1)! + 1 = (p-1) \times \underbrace{(p-2) \times \cdots \times 2}_{A} + 1.$$

Dans le terme A chaque élément x du produit va aller trouver son inverse y il vont se tenir la main pour former xy et ce produit disparaît pour donner 1. Comme on peut le faire pour tous les éléments de A, on a dans $\mathbb{Z}/p\mathbb{Z}$,

$$(p-1)! + 1 = (p-1) \times 1 + 1 = p = 0\ [p].$$

D'où le résultat.