Propriétés :

a) Soit $n \in \mathbb{N}^*$, on a la formule : $n = \sum_{d|n} \varphi(d)$.

b) Si p est un nombre premier alors $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

preuve :

a) On considère l'ensemble $A = \{\frac{1}{n}, \frac{2}{n}, \ldots, 1\}$ et pour tout diviseur d de n, on pose $A_d = \{\frac{k}{d}; k \in [\![1; d]\!], k \wedge d = 1\}$. Montrons tout d'abord que l'ensemble des A_d pour $d|n$ forme une partition de A. Tout éléments de A peut s'écrire sous la forme $\frac{k}{d}$ avec $k \wedge d = 1$ (c'est l'écriture sous forme de fraction irréductible) et réciproquement tout élément de A_d est élément de A. Il suffit donc de montrer que les A_d sont deux à deux disjoints.
Soient d et d' deux diviseurs distincts de n et soient $k \in [\![1; d]\!]$ et $k' \in [\![1; d']\!]$ tels que $k \wedge d = 1$ et $k' \wedge d' = 1$. Si $\frac{k}{d} = \frac{k'}{d'}$ alors $kd' = k'd$ donc $d'|k'd$ mais puisque $d' \wedge k' = 1$ d'après le lemme de Gauss $d'|d$. De manière tout à fait symétrique on a aussi $d|d'$ et donc $d = d'$, ce qui est absurde, les A_d sont donc deux à deux disjoints.

$$A = \bigsqcup_{d|n} A_d \qquad (\textit{union disjointe})$$

Soit en prenant le cardinal : $n = \sum_{d|n} Card(A_d)$ mais d'après la définition de A_d, on a :

$$n = \sum_{d|n} \varphi(d)$$

b) On pose $n = p - 1$ et soit d un diviseur de n. Supposons qu'il existe $x \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre d, alors $< x > \simeq \mathbb{Z}/d\mathbb{Z}$ et d'après le théorème de Lagrange tout $y \in < x >$ vérifie $y^d = 1$. Or le polynôme $X^d - 1$ admet au plus d racines dans le corps $\mathbb{Z}/p\mathbb{Z}$. En conclusion : tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ d'ordre d sont dans $< x >$, or on sait exactement combien il y a d'élément d'ordre d dans $\mathbb{Z}/d\mathbb{Z}$, c'est $\varphi(d)$.
Si on note $N(d)$ le nombre d'élément d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^*$, on vient de montrer que soit il existe un élément d'ordre d et alors $N(d) = \varphi(d)$ soit il n'en existe pas et alors $N(d) = 0$. Dans tous les cas $N(d) \leqslant \varphi(d)$.
$(\mathbb{Z}/p\mathbb{Z})^*$ peut être partionné selon l'ordre de ses éléments, on a alors d'après ce qui précède et a) :

$$n = \sum_{d|n} N(d) \leqslant \sum_{d|n} \varphi(d) = n$$

L'inégalité est alors en fait une égalité et $N(d) = \varphi(d)$ pour tout $d|n$. En particulier $N(n) = \varphi(n) \geqslant 1$, donc $(\mathbb{Z}/p\mathbb{Z})^*$ possède un élément d'ordre $n = p - 1$, il est donc cyclique et isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

José Gregorio : http://agregorio.net

Remarques :

1. Pour le a), il y a une méthode beaucoup plus classique qui consiste à démontrer que pour tout $d|n$ il existe un unique sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, il est isomorphe à $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$. Il vaut mieux avoir une idée de la démonstration car le jury pourra poser la question.

2. Une autre question que le jury pourrait éventuellement poser est : quelle est la structure de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ avec p premier et $\alpha \geqslant 2$? Réponse : si $p \geqslant 3$ alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$, sinon $(\mathbb{Z}/4\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z}$ et pour $\alpha \geqslant 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Thèmes abordés :

* Arithmétique
* Groupes cycliques
* Nombres premiers
* Divisibilité et indicatrice d'Euler
* Corps $\mathbb{Z}/p\mathbb{Z}$

Bibliographie :

La première partie se trouve dans "Les maths en tête, Algèbre" de Xavier Gourdon (ELLIPSES).
Pour la seconde partie et les remarques, on peut par exemple voir "Cours d'algèbre" de Daniel Perrin (ELLIPSES).

José Gregorio : http://agregorio.net