CARRÉS MODULAIRES

§1. Petites questions

1 Trouver un $x \in \mathbf{Z}$ tel que $x^2 \equiv -1\ [5]$.

2 Trouver *tous* les $x \in \mathbf{Z}$ tels que $x^2 \equiv -1\ [5]$. On justifiera soigneusement la réponse.

3 On dit que $a \in \mathbf{Z}$ est un carré modulo m s'il existe $x \in \mathbf{Z}$ tel que $x^2 \equiv a\ [m]$. On dit d'un tel x qu'il est une *racine carrée* de a (modulo m). Dans l'exercice précédent, on a montré que $a = -1$ est un carré (modulo $m = 5$). Donner d'autres exemples, pour différentes valeurs de a et m.

4 Est-ce que -1 est un carré (modulo 7) ?

5 Démontrer que pour tout $n \in \mathbf{N} - \{0\}$, le nombre $2n + 1$ est un carré (modulo n^2).

6 Démontrer que si $x \in \mathbf{Z}$ est un carré (au sens habituel) alors c'est un carré (modulo m) pour tout $m \in \mathbf{N} - \{0\}$.

7 Réciproquement, si $x \in \mathbf{Z}$ est un carré modulo m pour tous les $m \in \mathbf{N} - \{0\}$, est-ce un carré au sens habituel ?

§2. Approches naïves

§3. Détection des carrés

§4. Racines carrées