Introduction à la théorie de l'informatique

Répétition 2

Année académique 2011-2012

1. Soit $n \in \mathbb{N}$ tel que $n > 2$. Démontrez que s'il n'existe pas de nombre premier $p \leq \sqrt{n}$ qui divise n, alors n est un nombre premier.

2. Utilisez le théorème fondamental de l'arithmétique pour démontrer que pour tout $n \in \mathbb{N}$, $\sqrt{n}$ est irrationnel sauf si n est un carré parfait, c'est-à-dire sauf s'il existe $m \in \mathbb{N}$ tel que $n = m^2$.

3. Démontrez ou infirmez les propositions suivantes :
   (a) Soient $a, b \in \mathbb{Z}$, $c \in \mathbb{N}$ et $n \in \mathbb{N}_0$. Si $a \equiv b \pmod{n}$, alors $a^c \equiv b^c \pmod{n}$.
   (b) Soient $a, b \in \mathbb{N}$, $c \in \mathbb{Z}$ et $n \in \mathbb{N}_0$. Si $a \equiv b \pmod{n}$, alors $c^a \equiv c^b \pmod{n}$.

4. Soient p un nombre premier, k un multiple positif de $p - 1$, et

$$S = \sum_{i=1}^{p-1} i^k.$$

   Utilisez le théorème de Fermat pour démontrer que

$$S \equiv -1 \pmod{p}.$$