UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Devoir Maison

Sur le nombre de solutions d'une équation du second degré

Problème

Le but de ce problème est de montrer que l'équation $X^2+X+1=0$ *peut avoir un nombre arbitrairement grand de solutions dans les anneaux* $\mathbf{Z}/n\mathbf{Z}$.

Pour un nombre premier p, *on notera* $\mathbb{F}_p$ *le corps* $\mathbf{Z}/p\mathbf{Z}$. *On rappelle qu'alors le groupe* $(\mathbb{F}_p^\times, \times)$ *des inversibles de* $\mathbb{F}_p$ *est cyclique. On pourra admettre le résultat d'une question pour continuer.*

1 Si p est un nombre premier, combien au maximum l'équation $X^2+X+1=0$ a-t-elle de solutions dans l'anneau $\mathbf{Z}/p\mathbf{Z}$?

2 Déterminer les solutions de l'équation $X^2+X+1=0$

a dans $\mathbf{Z}/2\mathbf{Z}$, dans $\mathbf{Z}/2n\mathbf{Z}$.

b dans $\mathbf{Z}/7\mathbf{Z}$.

c dans $\mathbf{Z}/13\mathbf{Z}$.

d À l'aide des questions précédentes, déterminer les solutions de l'équation $X^2+X+1=0$ dans $\mathbf{Z}/91\mathbf{Z}$.

3 Soit p est un nombre premier plus grand que 5. Montrer que l'équation $X^2+X+1=0$ admet une solution dans le corps $\mathbb{F}_p$ si et seulement si l'équation $X^3=1$ admet une solution *différente de* 1 dans $\mathbb{F}_p$.

4 Soit p est un nombre premier plus grand que 5. Montrer que l'équation $X^2+X+1=0$ admet une solution dans le corps $\mathbb{F}_p$ si et seulement si $(\mathbb{F}_p)^\times$ a un élément d'ordre 3.

5 Soit p est un nombre premier plus grand que 5. Montrer que l'équation $X^2+X+1=0$ admet une solution dans le corps $\mathbb{F}_p$ si et seulement si p est congru à 1 modulo 3.

6 Soit p est un nombre premier plus grand que 5. Montrer que si l'équation $X^2+X+1=0$ admet une solution a dans le corps $\mathbb{F}_p$ elle admet une autre solution disctincte $-1-a$.

7 On admet qu'il existe une infinité de nombres premiers congrus à 1 modulo 3. Montrer que l'équation $X^2+X+1=0$ peut avoir un nombre arbitrairement grand de solutions dans les anneaux $\mathbf{Z}/n\mathbf{Z}$.