Université Paris Diderot
L2, MI4, Groupes et arithmétique, année 2008-2009

4 Structure multiplicative de $\mathbb{Z}/n\mathbb{Z}$. Équations modulaires linéaires

4.1 Calcul de puissances

1. Quel est le dernier chiffre de 7777^{7777} ?
2. Quels sont les restes des divisions euclidiennes de 900^{2000} et de $101^{102^{103}}$ par 13 ?
3. Quel est le reste de la division euclidienne de $31^{32^{33}}$ par 7 ?

4.2 Diviseurs premiers des nombres de Fermat

Soit $n \in \mathbb{N}$ et $F_n = 2^{2^n} + 1$ le n^{e} nombre de Fermat. Soit p un diviseur premier de F_n. Remarquer $2^{2^n} = -1 \mod p$, puis montrer que l'ordre de 2 dans $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est 2^{n+1}. En déduire qu'il existe $k \in \mathbb{N}$ tel que $p = 2^{n+1}k + 1$. Trouver un diviseur de $F_5 = 4\,294\,967\,297$. *Ce fut la démarche d'Euler pour réfuter la conjecture de Fermat, selon laquelle tous les nombres F_n sont premiers.*

4.3

Soit $n > 1$ un entier tel que $2^n = 1 \mod n$. Soit p le plus petit diviseur premier de n.

1. Montrer que $p > 2$.
2. Soit r l'ordre de 2 dans le groupe multiplicatif $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$. Montrer que $r > 1$ et que r divise n et $p - 1$.
3. Conclure qu'il n'existe pas de $n > 1$ tel que $2^n = 1 \mod n$.

4.4 Inverses dans $\mathbb{Z}/n\mathbb{Z}$

Rappeler à quelle condition un élément a est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Donner une procédure utilisant l'algorithme d'Euclide-Bezout pour calculer l'inverse d'un élément.

4.5

Résoudre les équations :

1. $x^2 + 4x - 1 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
2. $x^2 + 5x + 2 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
3. $x^2 + 6x - 13 = 0$ dans $\mathbb{Z}/21\mathbb{Z}$.
4. $x^2 + 4x + 6 = 0$ dans $\mathbb{Z}/9\mathbb{Z}$.

4.6 Calculs de $\phi(n)$ pour certaines valeurs de n

1. Calculer $\phi(n)$ pour $n \in \{5, 8, 13, 19, 21, 25, 27, 33, 36\}$.
2. Pour quelles valeurs de n, parmi ceux de la question 1, le groupe $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ est-il cyclique ?

4.7

Pour quels entiers n a-t-on $\phi(n) = \frac{n}{3}$?

4.8

1. Existe-t-il un entier $n > 1$ tel que $x^n \equiv 1 \bmod 15$ pour tout $x \in \mathbb{Z}$?
2. Trouver un entier $n > 1$ tel que $x^n \equiv 1 \bmod 15$ pour tout entier $x \in \mathbb{Z}$ premier avec 15.

4.9

Déterminer les entiers $x \in \mathbb{N}$ tels que $3^x \equiv 11 \bmod 14$.

4.10 Racines de -1 modulo p

Soit p un nombre premier différent de 2.

1. Montrer que p est de la forme $4k + 1$ ou $4k + 3$.
2. Vérifier que l'équation
$$x^2 + 1 \equiv 0 \bmod p \tag{1}$$
n'a pas de solution si p est de la forme $4k + 3$. *Indication :* déterminer l'ordre de x.
3. Si $p = 4k + 1$, vérifier que $x = (2k)!$ est solution de l'équation (1). *Indication :* utiliser le théorème de Wilson, $(p - 1)! \equiv -1 \bmod p$.
4. Exemple : donner les solutions de l'équation $x^2 + 1 \equiv 0 \bmod 13$.