MT 282
24/11/96

Université Paris 7
U.F.R. de Mathématiques
P. Perrin/B. Keller

# Exercices sur la structure multiplicative de $\mathbf{Z}/n\mathbf{Z}$

1) Quel est le reste dans la division par 17 de $2^{1996}$ ?

2) Trouver à quoi est congru $1995^{1995}$ modulo 23.

3) Soit $n$ un entier premier avec 10. Montrer qu'il admet un multiple dont l'écriture décimale ne comporte que des 1.

4) Montrer que les entiers de la forme $4 \times 14^k + 1$ (où $k$ est au moins égal à 1 ) ne sont pas premiers (on pourra les regarder modulo 3 ou 5).

5) Montrer que les entiers de la forme $521 \times 12^k + 1$ (où $k$ est au moins égal à 1 ) ne sont pas premiers (on pourra les regarder modulo 5, 13 ou 29).

6) Soit $2^n - 1$ un nombre de Mersenne. Montrer que, pour $n$ premier inférieur ou égal à 7, le nombre $2^n - 1$ est premier.

7) Considérons les deux nombres de Mersenne $2^{11} - 1$ et $2^{13} - 1$. Chercher les facteurs premiers possibles de ces deux nombres. On pourra tout d'abord majorer ces facteurs possibles par la racine carrée du nombre en question. Ensuite remarquer que, si $p$ divise $2^n - 1$, alors $2^n$ est congru à 1 modulo $p$ et que donc l'ordre de 2 divise $n$.

8) Trouver les facteurs premiers de $3^{12} - 1 = 531440$. On pourra opérer comme ci-dessus en ajoutant la recherche des facteurs premiers des nombres $3^d - 1$ où $d$ est un diviseur propre de 12.

9) Même exercice que ci-dessus avec le nombre $2^{35} - 1$.

10) (Il s'agit de la généralisation des exercices précédents) Soit $p$ un facteur premier du nombre $a^n - 1$ (où $a$ désigne un entier naturel supérieur ou égal à 2 ). Montrer que soit $p$ divise un nombre de la forme $a^d - 1$ (où $d$ est un diviseur de $n$ et $d$ est distinct de $n$), soit $p$ est congru à 1 modulo $n$. Montrer de plus que, si $p$ et $n$ sont impairs, le nombre $p$ est congru à 1 modulo $2n$.

11) Montrer que les quatre premiers nombres de Fermat (de la forme $2^a + 1$ où $a$ est une puissance de 2 ) sont égaux à 3, 5, 17 et 257 et sont premiers.

12) Soit $b$ un entier premier à $m$ (où $m$ est strictement supérieur à 2 ) et $a, c$ deux entiers naturels. Montrer que, si $b^a$ est congru à $-1$ modulo $m$ et $b^c$ est congru à $\pm 1$ modulo $m$, alors $b^d$ est congru à $-1$ modulo $m$ et $a/d$ est impair ($d$ désigne le pgcd de $a$ et $c$).

13) (suite) Si $p$ est un facteur premier de $b^n + 1$ alors soit $p$ divise un nombre de la forme $b^d + 1$ (où $d$ est un diviseur propre de $n$ et $n/d$ est impair), soit $p$ est congru à 1 modulo $2n$.

14) (application) Soit $m$ l'entier $2^{24} + 1$ (il vaut 16 777 217). Trouver un nombre premier de Fermat qui divise $m$. Montrer que tout autre facteur premier de $m$ est congru à 1 modulo 48.

15) Montrer que 341 divise $2^{341} - 2$ sachant que $341 = 11 \times 31$.

Dans les exercices suivants le fait que $(\mathbb{Z}/p\mathbb{Z})^*$ soit cyclique d'ordre $p-1$ ($p$ est supposé premier) n'est pas nécessaire. Ce résultat peut toutefois servir de guide dans la recherche d'une solution.

16) Trouver l'ordre de tous les éléments de $(\mathbb{Z}/29\mathbb{Z})^*$ (vu comme groupe multiplicatif). En déduire un isomorphisme explicite de ce groupe sur le groupe $(\mathbb{Z}/28\mathbb{Z}, +)$ .

17) Trouver toutes les solutions des équations suivantes :

$x^3 = 1$ dans $\mathbb{Z}/19\mathbb{Z}$ et

$x^4 = 1$ dans $\mathbb{Z}/17\mathbb{Z}$.

18) Discuter l'équation $x^3 = a$ dans $\mathbb{Z}/13\mathbb{Z}$ suivant les valeurs de l'élément $a$.

19) Résoudre l'équation $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = 0$ dans $\mathbb{Z}/29\mathbb{Z}$.

20) Montrer que la somme des carrés de $\mathbb{F}_p$ est congrue à 0 modulo $p$ dès que $p$ est au moins égal à 5.

En déduire que le nombre suivant

$$u_p = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

(où $p$ est un nombre premier) s'écrit

$$u_p = \frac{A_p}{B_p}$$

où $A_p$ et $B_p$ sont premiers entre eux et $A_p$ est divisible par $p^2$.

Les exercices suivants utilisent le fait qu'un élément est un carré dans $\mathbb{F}_p$ si et seulement si $x^{\frac{(p-1)}{2}}$ est égal à 1.

21) Montrer que $-1$ est une puissance quatrième dans $\mathbb{Z}/p\mathbb{Z}$ (où $p$ est premier) si et seulement si $p$ est congru à 1 modulo 8.

22) On cherche à étudier pour quels nombres premiers $p$ l'élément 2 est un carré dans $\mathbb{F}_p$. On va donc calculer $2^{\frac{(p-1)}{2}}$ modulo $p$. Soit $\zeta$ la racine huitième de l'unité donnée par $\exp(2\pi i/8)$.

a) Montrer que $\zeta$ vérifie les relations suivantes : $\zeta^2 = i$, $\zeta + \zeta^{-1} = \sqrt{2}$, $\zeta^2 + \zeta^{-2} = 0$ , $\zeta^3 + \zeta^{-3} = -\sqrt{2}$ et $\zeta^4 + \zeta^{-4} = -2$. En déduire que, si on note $y$ l'élément $\zeta + \zeta^{-1}$, on a $y^2 = 2$.

b) Comme $p$ est impair, on notera $h = (p-1)/2$ ou encore $p = 1 + 2h$. Vérifier que $y^p\zeta^p$ et $y^p\zeta$ sont éléments de $\mathbb{Z}[i]$. Montrer que $y^p\zeta^p$ est congru dans $\mathbb{Z}[i]$ à $1 + i^p$. En déduire que $y^{2h} \times (y\zeta)$ est congru à $i^{-h} + (-1)^h i^{1-h}$ modulo $p$ dans $\mathbb{Z}[i]$.

c) Utiliser ce qui précède pour évaluer $2^{(p-1)/2} = y^{p-1} = y^{2h}$ modulo $p$. En conclure que 2 est un carré modulo $p$ si et seulement si $p$ est congru à $\pm 1$ modulo 8.

Voici une autre démonstration du résultat ci-dessus.

23) Supposons que $p$ soit premier et congru à 1 modulo 8. On pose $p = 1 + 8m$.

a) En écrivant, dans le produit $A = 2.4.\cdots 4m.(4m+2).\cdots(8m-2).8m$, les entiers $4m+2, \cdots, 8m$ sous la forme $p-(4m-1-2h)$ (où $h$ varie entre 0 et $2m-1$ ) montrer que $A = 24m(4m)!$.

b) Remarquer que, pour la même raison, $A$ est congru à $(4m)!$ modulo $p$.

c) En conclure que 2 est un carré modulo $p$ .

Pour mémoire voici un exercice d'une liste précédente.

24) Il s'agit dans cet exercice de montrer que $-3$ est un carré modulo $p$ si $p$ est un nombre premier dans $\mathbb{Z}$ congru à 1 modulo 3 . Nous avons utilisé ce résultat dans le cours pour établir la liste des nombres premiers dans $\mathbb{Z}[j]$.

Soit $p$ un nombre premier dans $\mathbb{Z}$ congru à 1 modulo 3. Remarquer que p est nécessairement impair. On sait que $-3$ est un carré dans $\mathbb{F}_p$ si et seulement si $a = (-3)^{\frac{(p-1)}{2}}$ est égal à 1 modulo $p$ (voir le cours). Nous allons calculer $a$. Montrer que $-3 = (2j+1)^2$. Montrer que $a$ est congru à 1 modulo $p$ dans $\mathbb{Z}[j]$ donc dans $\mathbb{Z}$.

L'exercice suivant porte sur le cinquième nombre de Fermat. On note $F_5$ ce nombre. Il vaut $2^{32}+1$ puisque $2^5 = 32$. On notera $p$ un facteur premier (à priori quelconque) de $F_5$. Au fait on a

$$F_5 = 4\ 294\ 967\ 296 + 1 = 4\ 294\ 967\ 297.$$

25) a) En reprenant les notations précédentes montrer que 2 est d'ordre $2^6$ dans $\mathbb{F}_p$. En conclure que $p$ est congru à 1 modulo $2^6$.

b) En utilisant l'exercice 22 ou 23 remarquer que $2^{\frac{(p-1)}{2}}$ est congru à 1 modulo $p$. En conclure que $\frac{(p-1)}{2}$ est divisible par $2^6$ et que $p$ est congru à 1 modulo $2^7$.

c) En recherchant les nombres premiers de la forme $1 + k \times 2^7 = 1 + 128k$, montrer que pour $k = 5$ on obtient le nombre 641 qui est un facteur de $F_5$. Le quotient valant 6 700 417. [Ce dernier résultat fut remarqué par Euler en 1732]

d) Remarquer que $(1 + 21 \times 128)^2$ est supérieur à 6 700 417. En cherchant les nombres premiers de la forme $1 + 128k$ où $k$ varie entre 1 et 20, montrer qu'aucun ne divise 6 700 417. En conclure que ce dernier nombre est premier. [Euler avait aussi démontré ce résultat]