MT 282
23/09/96

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

Exercices d'arithmétique élémentaire

Exercices sur les anneaux $\mathbf{Z}/n\mathbf{Z}$

1) Résoudre dans $\mathbf{Z}/5\mathbf{Z}$ le système suivant

$$\begin{aligned} x + 2\,y &= 3 \\ 2\,x + 3\,y &= 4 \end{aligned}$$

2) Résoudre dans $\mathbf{Z}/5\mathbf{Z}$ le système suivant où a est un paramètre.

$$\begin{aligned} x + 2\,y &= a \\ 2\,x - y &= 1 \end{aligned}$$

3) Résoudre dans $\mathbf{Z}/6\mathbf{Z}$ le système suivant (on discutera suivant les valeurs de a et b).

$$\begin{aligned} 5\,x + 2\,y &= a \\ 2\,x + 4\,y &= b \end{aligned}$$

Exercices sur la notion de divisibilité.

4) Trouver la plus grande puissance de 2 divisant 1000! (il est raisonnable de trouver 994). Généraliser à un autre nombre premier comme 3 par exemple. Puis généraliser à $n!$. Trouver le nombre de zéros figurant à la fin de l'écriture décimale de 1000! .

5) Trouver le nombre de solutions (en entiers naturels) de $n = x + 2\,y$, où n est un paramètre et x, y les inconnues.

6) Montrer que le nombre suivant

$$u_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$$

ne peut être entier. On pourra montrer par récurrence (en utilisant deux formules de récurrence différentes suivant que n est pair ou impair) qu'il s'écrit

$$u_n = \frac{2\,p_n + 1}{2\,q_n}.$$

7) Montrer que le nombre suivant

$$u_1 = 1 + \frac{1}{2} + \ldots + \frac{1}{p-1}$$

(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. (On peut montrer en fait que A_p est divisible par p^2 ; on le fera dans une prochaine feuille d'exercices).

8) Soit n un entier naturel non nul. Soit p un diviseur premier de n et soit a l'exposant de la plus grande puissance de p divisant n . Soit b un entier naturel inférieur ou égal à a . Montrer que $a - b$ est l'exposant de la plus grande puissance de p divisant le coefficient binomial

$$C_n^{p^b}.$$

Exercices nécessitant la division euclidienne ou la structure de corps sur les F_p

9) Onze personnes décident de se réunir régulièrement à dîner autour d'une table ronde (ou ovale!). Chaque personne fait, à cette occasion, la connaissance de ses deux voisins. Trouver (au moins) une stratégie pour qu'au bout de cinq repas chacun ait fait la connaissance des dix autres personnes.

10) Résoudre l'équation $x^2 - 4\,x - 2 = 0$ dans $\mathbf{Z}/5\mathbf{Z}$. Même question pour les deux équations suivantes: $x^2 - 2\,x + 2 = 0$ et $x^2 - 4\,x - 3 = 0$.

11) Soient a et b deux nombres premiers entre eux. Montrer que le PGCD des deux nombres $a + b$ et $a - b$ est nécessairement un diviseur de 2 . Préciser quand cela peut être 2 .

12) Soit a un entier relatif. Montrer que le PGCD de a et $a + k$ (où k est un entier supérieur ou égal à 1) divise k.

Exercices sur la rationalité

13) Montrer que

$$\sqrt[n]{m}$$

est un rationnel si et seulement si m est une puissance n-ième dans $\mathbf{Z}$.

14) Montrer que $\log_{10}(2)$ est irrationnel.

15) Montrer que

$$\sqrt{2} + \sqrt{3}$$

est solution de l'équation $x^4 - 10x^2 + 1 = 0$. Chercher toutes les racines rationnelles de cette équation. Qu'en concluez vous pour $\sqrt{2} + \sqrt{3}$?

16) Vérifier que le nombre

$$\sqrt[3]{20+14\sqrt{2}}+\sqrt[3]{20-14\sqrt{2}}$$

est rationnel.

17) Montrer que l'équation $3\,x^2+2=y^2$ n'a pas de solutions dans l'anneau $\mathbf{Z}$. Même question pour l'équation $7\,x^2+2=y^3$.

18) Nous allons résoudre complètement l'équation $x^2+y^2=z^2$ où x, y et z sont des entiers relatifs.

a) Si (x,y,z) est un triplet solution, montrer qu'il s'écrit (dx',dy',dz') où d est élément de $\mathbf{Z}$ et x', y' et z' sont premiers deux à deux.

b) Supposons que le triplet (x,y,z) soit solution et soit formé d'entiers premiers deux à deux. Montrer que x et y n'ont pas la même parité.

c) Sous les hypothèses précédentes (cf. b) prenons x pair. Montrer que l'on peut écrire $y=u-v$ et $z=u+v$ où u et v sont des entiers premiers entre eux.

d) Sous les hypothèses de c) montrer que u et v sont les carrés de deux entiers premiers entre eux.

e) Conclure. (Cette équation est un des cas triviaux de l'équation de Fermat. Nous essaierons de résoudre également le cas de l'exposant 3 et celui de l'exposant 4).

19) Montrer que la congruence $x^2\equiv 1\ (2^b)$ a une solution si b est égal à 1 , deux solutions si b est égal à 2 et quatre solutions si b est supérieur ou égal à 3.

20) Montrer que 30 divise n^5-n quel que soit $n\in\mathbf{N}$. Montrer de même que 42 divise n^7-n quel que soit n.

Exercices sur l'identité de Bezout et le calcul des inverses dans F_p

21) Les nombres 1017 et 269 sont-ils premiers entre eux? Donner une identité de Bezout entre ces deux nombres. Trouver toutes les identités de Bezout entre ces deux nombres. L'élément 269 a-t-il un inverse dans $\mathbf{Z}/1017\mathbf{Z}$?

22) Résoudre le système de congruences suivant

$$\begin{aligned} x &\equiv 1\ (7)\\ x &\equiv 4\ (9)\\ x &\equiv 5\ (5) \end{aligned}$$

(on pourra tout d'abord chercher une identité de Bezout entre 5 et 63, 7 et 45 puis enfin 9 et 35).

23) Résoudre les équations $398\,u+600\,v=2$, $1841\,u+3647\,v=1$ où u et v sont des variables entières.

24) Résoudre l'équation $323x+391y+437z = 10473$ où x, y et z sont des variables entières.

25) Soient deux entiers n et m . Montrer que le produit mn est égal au produit de leur PGCD et de leur PPCM.

Exercices sur les nombres premiers.

26) Montrer que, si $a^n - 1$ est un nombre premier, alors a est pair et égal à 2 et que n est premier (on pourra utiliser l'égalité remarquable donnant $x^n - y^n$). De tels nombres s'appellent nombres de Mersenne. C'est une question sans réponse à ce jour de savoir s'ils sont en nombre infini.

27) Montrer que, si $a^n + 1$ est un nombre premier, alors a est pair et que n est une puissance de 2 (on pourra utiliser l'égalité remarquable donnant $x^n + y^n$ lorsque n est impair). Donner un exemple de nombre premier de cette forme pour lequel a est différent de 2. De tels nombres s'appellent nombres de Fermat lorsque a est égal à 2 . C'est une question sans réponse à ce jour de savoir si ceux d'entre eux qui sont premiers, sont en nombre infini.

28) Montrer que, si un entier n n'est divisible par aucun facteur premier p inférieur à sa racine cubique, il est premier ou produit de deux facteurs premiers.

29) Soient p et q deux entiers premiers impairs consécutifs. Montrer que $p+q$ admet une décomposition en au moins trois facteurs premiers (non nécessairement distincts).

30) Nous allons montrer que l'équation $x^4 + y^4 = z^4$ n'admet pas de solutions entières (x, y, z) non triviales (i.e. avec $xyz \neq 0$). En fait nous allons montrer le même résultat pour l'équation $x^4 + y^4 = z^2$. Raisonnons par l'absurde. Soit u le plus petit entier pour lequel il existe des entiers x et y non nuls tels que $x^4 + y^4 = u^2$.

   a) Montrer que x et y sont premiers entre eux, que u est impair et que, entre x et y , l'un est impair et l'autre pair.

   b) Supposons désormais x pair et y impair. Utiliser un exercice précédent pour écrire $x^2 = 2ab$, $y^2 = a^2 - b^2$ et $u = a^2 + b^2$ (où a et b sont premiers entre eux). Montrer que b est nécessairement pair et a impair (on pourra raisonner modulo 4).

   c) On pose donc $x = 2x'$ et $b = 2d$. Montrer que $a = a'^2$ et $d = d'^2$ et que a' et d' restent premiers entre eux.

   d) Appliquer à nouveau le même exercice précédent à l'identité obtenue pour y^2 soit $(2d'^2)^2 + y2 = (a'^2)^2$. En déduire une identité $a^4 + b^4 = a'^2$ où a' est inférieur strictement à u.