Arithmétique

(trois semaines)

(du lundi 13 novembre 2017 au vendredi 1er décembre 2017)

On note $a \wedge b$ le pgcd de a et b.

Exercice 1

Soit $(a, b, d) \in \mathbb{Z}^3$.

Montrer que : $\big(d \,|\, a \text{ et } d \,|\, b\big) \Longrightarrow \forall (u, v) \in \mathbb{Z}^2\,,\ d \,|\, au + bv$.

Exercice 2

Soit $n \in \mathbb{N}^*$. Montrer que le produit de n entiers naturels consécutifs est divisible par $n!$.

Exercice 3

Déterminer en utilisant l'algorithme d'Euclide $48 \wedge 27$ et $9100 \wedge 1848$.

Exercice 4

Soient a et b deux entiers naturels non nuls et $d = a \wedge b$.

Montrer qu'il existe $(a', b') \in \mathbb{N}^{*2}$ tel que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.

Exercice 5

Soit $(a, b, c) \in \mathbb{Z}_*^3$.

1. Montrer que : $a \wedge b = 1 \Longleftrightarrow \exists (u, v) \in \mathbb{Z}^2\,,\ au + bv = 1$.
2. Montrer qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$.
3. Montrer que : $\big(a \wedge b = 1 \text{ et } a \wedge c = 1\big) \Longleftrightarrow a \wedge (bc) = 1$.

Exercice 6

Soit $(a, b, c) \in \mathbb{N}^{*3}$.

1. Montrer que : $\big(c \,|\, a \text{ et } c \,|\, b\big) \Longleftrightarrow c \,|\, a \wedge b$.
2. En déduire que $ac \wedge bc = (a \wedge b)c$.

Exercice 7

Soit $(a, b) \in \mathbb{N}^2$. Montrer que : $(a + b)$ et ab premiers entre eux $\Longleftrightarrow$ a et b premiers entre eux.

Exercice 8

1. Via l'algorithme d'Euclide, déterminer une solution particulière de l'équation $71x + 19y = 2$.
2. En utilisant obligatoirement le théorème de Gauss, déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $71x + 19y = 2$.

Exercice 9

1. Via l'algorithme d'Euclide, déterminer une solution particulière de l'équation $134x + 56y = 4$.
2. En utilisant obligatoirement le théorème de Gauss, déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $134x + 56y = 4$.

Exercice 10

1. Soit $(p, q) \in \mathbb{Z}^2$ tel que $p \wedge q = 1$. Montrer que $p \wedge q^3 = 1$ et $p^3 \wedge q = 1$.
2. Soient $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, $P(X) = a_3X^3 + a_2X^2 + a_1X + a_0$ et $x = \dfrac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$. Montrer que si x est une racine de P alors p divise a_0 et q divise a_3.
3. Montrer que le polynôme $P(X) = X^3 + X - 3$ n'a pas de racine rationnelle c'est-à-dire n'a pas de racine de la forme $\dfrac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$.

Exercice 11

Soit $p \geqslant 5$ un nombre premier.

1. Montrer que $2 \mid p - 1$ et $2 \mid p + 1$.
2. En déduire que $8 \mid p^2 - 1$.
3. Soit $(a, b, c) \in \mathbb{N}^3$ tel que $a \mid b$ ou $a \mid c$. Montrer que $a \mid bc$.
4. En déduire que $3 \mid p^2 - 1$.
5. Soit $(a, b, c) \in \mathbb{N}^3$ tel que $a \mid c$, $b \mid c$ et $a \wedge b = 1$. Montrer que $ab \mid c$.
6. Déduire des questions précédentes que $24 \mid p^2 - 1$.

Exercice 12

Soit $(n, d, k) \in \mathbb{N}^3$ tel que $n \geqslant 2$, $d \geqslant 1$ et $k \geqslant 1$.

1. Justifier que
$$2^{dk} - 1 = \left(2^d - 1\right)\left(1 + 2^d + \left(2^d\right)^2 + \cdots + \left(2^d\right)^{k-1}\right)$$
2. Montrer que $2^n - 1$ premier $\Longrightarrow$ n premier.

   N.B. : on pourra démarrer cette question en prenant un diviseur d de n et on montrant que $d = 1$ ou $d = n$.

Exercice 13

Soient $n \in \mathbb{N}$ tel que $n \geqslant 2$ et $p \in \mathbb{N}$ le plus petit diviseur de n tel que $p \geqslant 2$.

1. Montrer que p est un nombre premier (on pourra raisonner par l'absurde).
2. Supposons que n n'est pas un nombre premier. Montrer que $2 \leqslant p \leqslant \sqrt{n}$.
3. Via les deux questions précédentes, montrer que si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier.
4. Via la question précédente, déterminer si 137 est un nombre premier.

Exercice 14

Soient $a = 256$ et $b = 5040$.

1. Décomposer a et b en produit de facteurs premiers.
2. En déduire $a \wedge b$.

Exercice 15

1. Combien 30^2 et 225^2 ont-ils de diviseurs positifs ?
2. Montrer qu'un carré parfait a toujours un nombre impair de diviseurs positifs.

Exercice 16

Soit $n \in \mathbb{N}$. Montrer (sans récurrence) que $3^{2n+1} + 2^{n+2}$ est divisible par 7.

Exercice 17

Soit $n \in \mathbb{N}$. Montrer que $3^{n+3} - 4^{4n+2}$ est divisible par 11.

Exercice 18

Déterminer le reste de la division euclidienne par 7 du nombre $a = 247^{349}$.

Exercice 19

Quel est le reste de la division euclidienne de 12^{1527} par 5 ?

Exercice 20

Soit p un nombre premier.

1. Soit k un entier tel que $0 < k < p$. Montrer que p divise C_p^k.
2. Soit $(a, b) \in \mathbb{Z}^2$. Montrer que
$$p \mid (a+b)^p - a^p - b^p$$
3. En déduire que
$$\forall m \in \mathbb{N}, \quad p \mid m^p - m$$
4. Montrer que si m et p sont premiers entre eux,
$$p \mid m^{p-1} - 1$$
5. Montrer que pour tout $n \in \mathbb{N}$, $n^p \equiv n\,[p]$ (petit théorème de Fermat).
6. Montrer que pour tout $n \in \mathbb{N}$, $(p \nmid n \Longrightarrow n^{p-1} \equiv 1\,[p])$.

Exercice 21

On se donne deux nombres premiers p et q distincts et on pose $n = pq$.

Soient $t \in \mathbb{N}$, c et d deux entiers naturels tels que $cd \equiv 1\big[(p-1)(q-1)\big]$.

1. Montrer que $p \mid t$ ou $p \wedge t = 1$.
2. Montrer, via le petit théorème de Fermat, que $t^{cd} \equiv t[p]$ et $t^{cd} \equiv t[q]$.
3. En déduire que $t^{cd} \equiv t[n]$.

   N.B. : cet exercice est utile en cryptographie. Il est à la base de la méthode RSA (inventée par Rivest, Shamir et Adleman en 1977). Voici le principe. Pour crypter un message, on choisit deux (très grands) nombres premiers p et q et on note $n = pq$. On cherche ensuite deux entiers naturels c et d tels que $cd \equiv 1\big[(p-1)(q-1)\big]$.
   Les messages t sont des entiers naturels dans $[\![0, n-1]\!]$.
   On code chacun de ces entiers en déterminant l'entier naturel a, appartenant à $[\![0, n-1]\!]$, vérifiant $t^c \equiv a[n]$.

   On décode chacun de ces entiers en déterminant l'entier naturel b, appartenant à $[\![0, n-1]\!]$, vérifiant $t^d \equiv b[n]$. [1]

   En notant $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, l'application $g : \mathbb{Z}_n \to \mathbb{Z}_n$ où $g(t) = t^c$ s'appelle une fonction de chiffrement et l'application $f : \mathbb{Z}_n \to \mathbb{Z}_n$ où $f(t) = t^d$ s'appelle une fonction de déchiffrement. L'exercice affirme que $f \circ g(t) = t$. On peut donc chiffrer un message (représenté par un élément $t \in \mathbb{Z}_n$) par le biais de l'application g, puis on le déchiffre par le biais de l'application f. Pour chiffrer un message, on doit connaître le couple (n, c), appelé la clef publique car elle est connue de tous. Pour déchiffrer, il faut connaître n et l'entier d appelé la clef secrète car elle n'est connue que de la personne qui reçoit le message codé.

1. Pour trouver a et b, on peut utiliser le logiciel libre Xcas (cf. `http://www-fourier.ujf-grenoble.fr/~parisse/giac/doc/fr/casrouge/`).

La sécurité de ce système repose sur le fait que connaissant la clef publique, il est très difficile de déterminer d : il faudrait par exemple factoriser n pour trouver p et q, ce qui est presque impossible de nos jours lorsque p et q sont grands, typiquement de l'ordre de 500 chiffres. En d'autres termes, tout le monde peut chiffrer mais seuls ceux connaissant la clef secrète peuvent déchiffrer.

Prenons un exemple.

Les lettres de l'alphabet sont chiffrées de la manière suivante :

A	B	C	D	···	Z
01	02	03	04	···	26

Lise a pour clef publique (n, c) avec $n = pq$ où $p = 3$ et $q = 13$.
On a donc $(p-1)(q-1) = 24$.

Elle peut donc choisir $c = 29$ et $d = 5$ car $cd = 145 \equiv 1[24]$.

Elle reçoit le message crypté suivant : 28 01 12 21 11 12 03 28 05

En utilisant le logiciel Xcas, on obtient le tableau suivant :

28	01	12	21	11	12	03	28	05
19	01	12	21	20	12	9	19	05

Il est donc à présent aisé de déchiffrer à partir de la deuxième ligne du tableau : « SALUT LISE ».