

ED n° 2 – Éléments d'arithmétique

Exercice 1

1° Décomposer 1155 en facteurs premiers.

2° A partir de là, donner l'ensemble des diviseurs de 1155.

3° Dessiner le diagramme de Hasse de l'ensemble des diviseurs de 1155 ordonné par la relation d'ordre de divisibilité.

Exercice 2

1. En utilisant l'algorithme d'Euclide, calculer les PGCD des couples (a, b) suivants :

a	b
43	16
44 231	2 750
6 234	3 312

2. En déduire le PPCM de 6 234 et 3 312.

Exercice 3

Une machine emballe des pièces dans des sacs, toutes identiques, de même que les sacs. La machine remplit les sacs, sauf si elle n'a pas assez de pièces pour le faire. Quand elle emballe 7 912 pièces le dernier sac n'est pas rempli et il contient 37 pièces. Quand elle en emballe 59 167 le dernier sac n'est toujours pas rempli mais cette fois il contient 42 pièces. Combien chaque sac contient-il de pièces ?

Exercice 4

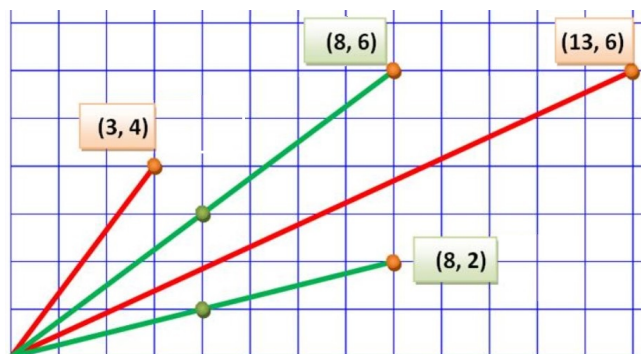
1. Décomposer en facteurs premiers les nombres suivants : 111, 6 788, 9 551 616.
2. Utiliser ces décompositions pour déterminer le PGCD de 6 788 et 9 551 616.

Exercice 5 – Nombres premiers entre eux

4. On rappelle que deux nombres sont premiers entre eux lorsque leur PGCD vaut 1. Parmi les couples de nombres suivants, indiquez (sans justification) ceux constitués de deux nombres premiers entre eux :

(3, 4) (8, 6) (13, 6) (8, 2)

En vous appuyant sur le graphique ci-contre, proposez une méthode graphique pour déterminer si deux nombres sont premiers entre eux (Indication : intéressez-vous au quadrillage).



Exercice 6 Crible d'Eratosthène

Il s'agit de trouver les nombres premiers inférieurs ou égaux à un entier N .

On met dans une table T les entiers de 2 à N . Ensuite, on enlève de T les multiples de 2. Puis dans la table T restante, on enlève les multiples de 3. On procède ainsi de suite. On s'arrête dès qu'on atteint un entier supérieur à la racine de N .

En appliquant l'algorithme d'Eratosthène, calculer les nombres premiers inférieurs ou égaux à 50.

Exercice 7 Inverse modulo

Soient les couples (e, p) de nombres premiers entre eux :

e	p
21	149
48	5

1° Rappeler la définition de l'inverse de e modulo p .

2° Calculer l'inverse de e modulo p pour les e et p précédents par l'algorithme d'Euclide étendu (i.e. avec « remontée » de l'algorithme). On fournira un $d > 0$.

Exercice 8 – Cryptographie : algorithme RSA

On considère $p = 17$, $q = 11$ deux nombres premiers. Ensuite, on pose $n = pq = 187$. On choisit $e = 7$ premier avec $(p - 1)(q - 1) = 160$.

1° Trouver d l'inverse de e modulo $(p - 1)(q - 1)$. On prendra $0 < d < (p - 1)(q - 1)$.

On considère le message \mathbf{M} suivant :

$$\mathbf{M} = \ell \square \mathbf{math}$$

Soit le codage des lettres suivant :

lettre	\square	a	b	c	d	e	f	g	h	i	j	k	ℓ	m	...	z
code	00	01	02	03	04	05	06	07	08	09	10	11	12	13	...	26

2° En utilisant la convention de codage précédente, transformer \mathbf{M} en chiffres. Découper \mathbf{M} en blocs de 3 chiffres. On s'assurera que chacun des blocs est inférieur à n .

3° A partir de la clé publique (n, e) , coder chacun des blocs.

4° Décoder ensuite ces blocs codés en utilisant n et la clé secrète d . Mettre les blocs décodés les uns à la suite des autres et retrouver le message \mathbf{M} .

5° A l'aide de la clé publique $n = 187$ et $e = 7$, Alice vous a envoyé le message suivant codé par blocs de 3 digits : 037020095144.

Quel est ce message ?

Exercice 9 – Equation diophantienne

1° Soit l'équation $ax = by + c$ avec a, b, c entiers. On recherche les solutions x, y entières. Montrer que si x_0, y_0 est solution, il en est de même pour $x_0 + kb, y_0 + ka$ pour tout k entier.

2° On considère l'équation $25x = 31y - 1$ avec x et y entiers. Remarquant que 25 et 31 sont premiers entre eux, utiliser l'algorithme d'Euclide (étendu) pour résoudre cette équation.

3° Alice change sa clé tous les 25 jours. Bob change sa clé tous les 31 jours. Sachant qu'Alice a changé sa clé aujourd'hui et que Bob a changé sa clé 3 jours auparavant, on voudrait savoir dans combien de jours Alice et Bob changeront de clé au même moment.

- a. Poser l'équation qui permet de répondre à la question.
- b. En utilisant, le résultat de la question précédente 2°, résoudre l'équation.
- c. De même, déterminer quand aura lieu la deuxième synchronisation.