CHAP 04 Arithmétique - Exercices

▸ **Intro**

Il s'agit ici d'exercices de base, afin de maîtriser les compétences et techniques de base.
Les exercices *en situation* sont prévus pour la suite de la fiche d'exercices !

Exercice 1 (★☆☆☆)

Écrire la division euclidienne de :

1. 425 par 4 ; 2. 1 001 par 9 ; 3. 7 297 par 26 ; 4. 427 par 401.

Exercice 2 (★☆☆☆)

Déterminer, en justifiant, si les entiers suivants sont premiers :

1. 1 789 ; 2. 503 ; 3. 483.

Exercice 3 (★☆☆☆)

1. Déterminer la décomposition en produit de facteurs premiers de :
   a. 88 ; b. 221 ; c. 117 000.
2. Déterminer, en détaillant la démarche, la liste des diviseurs de :
   a. 88 ; b. 221 ; c. 396.

Exercice 4 (★☆☆☆)

1. Par la méthode de votre choix, déterminer le PGCD des entiers suivants :
   a. 96 et 728 ; b. 1 071 et 2 200 ; c. 657 et 405.
2. Les entiers suivants sont-ils premiers entre eux ? Justifier.
   a. 8 753 et 147 ; b. 54 865 et 44 685.

Exercice 5 (★☆☆☆)

1. Compléter les congruences suivantes :
   a. $352 \equiv \ldots\ [7]$; b. $367 \equiv \ldots\ [15]$; c. $147 \equiv \ldots\ [8]$; d. $781 \equiv \ldots\ [10]$; e. $842 \equiv \ldots\ [5]$; f. $57 \equiv \ldots\ [13]$.
2. Compléter par le plus petit entier positif :
   a. $120 \equiv \ldots\ [7]$; b. $45 \equiv \ldots\ [7]$.
3. En utilisant les propriétés des congruences et les résultats de la question précédente, compléter :
   a. $240 \equiv \ldots\ [7]$; b. $120^2 \equiv \ldots\ [7]$; c. $120 + 45 \equiv \ldots\ [7]$; d. $3 \times 120 + 45 \equiv \ldots\ [7]$; e. $210 \equiv \ldots\ [7]$; f. $45^2 \equiv \ldots\ [7]$.

Exercice 6 (★★☆☆)

1. a. Réduire 287 modulo 11.
   b. En déduire que $287^{500} \equiv 1\ [11]$.
2. a. Simplifier les congruences $39 \equiv \ldots\ [7]$ et $25 \equiv \ldots\ [7]$.
   b. En déduire une réduction modulo 7 de $39^{200} - 25^{200}$, autrement dit $39^{200} - 25^{200} \equiv \ldots\ [7]$.
   c. Justifier que $39^{200} - 25^{200}$ est divisible par 7.

Licence Ouverte Etalab 2.0

▸ **Intro**

Les exercices d'arithmétique ne sont pas, en général, forcément les plus simples qui existent, mais en SIO les compétences mises en jeu sont classiques, et il suffit souvent de **bien lire** les énoncés et de savoir trouver (à la calculatrice éventuellement) des choses simples comme une **congruence**, un **reste**, un **PGCD**, une décomposition, etc

Exercice 7 (★★☆☆)

Une start-up conçoit un petit jeu gratuit pour smartphones.
Dans ce jeu, un personnage est généré à chaque début de partie avec un équipement choisi dans une liste de 40 objets, vêtements et accessoires, qui sont numérotés de 0 à 39.
Le concepteur du jeu envisage différents algorithmes pour attribuer automatiquement ces objets à chaque début de partie. Le but de cet exercice est d'étudier certains d'entre eux.

1. Décomposer 40 et 12 en produits de facteurs premiers.
2. Calculer le PGCD de 12 et 40.
3. Le concepteur du jeu envisage d'attribuer les objets à chaque début de partie en parcourant la liste de leurs numéros par des sauts d'amplitude constante a, où a est un nombre entier strictement positif :
   - lors de la première partie, le personnage se voit attribuer l'objet numéro 0 ;
   - pour obtenir le numéro de l'objet à partir de la deuxième partie, on ajoute a au numéro précédent et on calcule le reste de cette somme dans la division euclidienne par 40. Le reste obtenu est alors le numéro attribué à l'objet.

   Par exemple, en choisissant la valeur $a = 12$, la liste des numéros des objets dans l'ordre est :

   $$0\,;\,12\,;\,24\,;\,36\,;\,8\,;\ldots$$

   a. Compléter la liste des numéros des objets attribués lors des 11 premières parties, pour une amplitude de saut égale à 12.
   b. Ce choix d'amplitude permet-il d'utiliser tous les objets au cours des parties successives ?
4. On admet le résultat suivant :

   « Le nombre a choisi permet de former une liste complète comportant tous les numéros de 0 à 39 dans le cas où le PGCD de 40 et de a est égal à 1, et dans ce cas seulement ».

   Ainsi, les nombres a permettant d'utiliser tous les objets au cours des parties successives sont les entiers a qui sont premiers avec 40.

   Donner la liste de tous les entiers a compris entre 1 et 39 pour lesquels, au cours des parties successives, tous les objets seront utilisés.

Exercice 8 (★★★☆)

Alice souhaite que Bob lui envoie des données confidentielles par Internet. Pour éviter que ces données puissent être exploitées par une tierce personne, ils ont recours à un cryptage de type RSA.
Aucune connaissance sur le cryptage RSA n'est attendue dans cet exercice.

Partie A - Création des clés publique et privée par Alice

1. Il faut tout d'abord choisir deux nombres premiers distincts notés p et q, puis calculer leur produit noté n. Alice décide de prendre $p = 5$ et $q = 23$, ce qui donne $n = 115$.

   Expliquer pourquoi 23 est un nombre premier.
2. Il faut ensuite calculer $K = (p-1) \times (q-1)$, ce qui donne ici $K = 4 \times 22 = 88$, puis trouver un entier naturel c, compris entre 2 et K, qui soit premier avec K. Le couple d'entiers $(n\,;\,c)$ est la clé publique. Alice décide de prendre $c = 9$.
   a. Donner la décomposition en produit de facteurs premiers de 88.
   b. Expliquer pourquoi 9 et 88 sont deux nombres premiers entre eux.
3. Il faut enfin trouver un entier d tel que $d \times c \equiv 1 \ [K]$. Le couple d'entiers $(n\,;\,d)$ est la clé privée. Alice a trouvé $d = 49$.

   Expliquer pourquoi $49 \times 9 \equiv 1 \ [88]$.

Partie B - Cryptage du message à envoyer par Bob avec la clé publique d'Alice

Alice envoie sa clé publique à Bob et celui-ci s'en sert pour crypter un nombre a, qui doit être un entier naturel strictement inférieur à n. Le nombre crypté b est alors égal au reste dans la division euclidienne de a^c par n. C'est ce nombre crypté b que Bob envoie à Alice.
Bob veut transmettre à Alice le nombre 12.
Déterminer le nombre crypté b que Bob envoie à Alice.

Partie C - Décryptage d'un message reçu par Alice avec sa clé privée

Cette partie est indépendante de la précédente.
Alice reçoit un nouveau nombre crypté de la part de Bob : le nombre 2. Pour le décrypter, Alice utilise sa clé privée, c'est-à-dire le couple $(n\,;\,d)$.
On admet que le nombre non crypté transmis par Bob, noté a, est égal au reste dans la division euclidienne de 2^{49} par n.
Alice doit donc calculer le reste dans la division euclidienne de 2^{49} par 115 pour trouver a.
Mais sa calculatrice ne permet pas de calculer la valeur exacte de 2^{49}. Cependant, elle a pu obtenir :

$$2^{33} = 8\,589\,934\,592 \text{ et } 8\,589\,934\,592 \equiv 47 \ [115],$$

$$2^{16} = 65\,536 \text{ et } 65\,536 \equiv 101 \ [115].$$

À partir de ces résultats, calculer le nombre a transmis par Bob à Alice.

Exercice 9 (★★☆☆)

Pour une authentification, le serveur d'une entreprise envoie à un utilisateur un mot de passe codé qu'il devra décoder.

Le serveur de l'entreprise code un mot de passe de la façon suivante :

- à chaque lettre de l'alphabet, on associe son rang x selon le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	13	14	15	16	17	18	19	20	21	22	23	24	25

- on fixe une clé $(a\,;\,b)$, où a et b sont deux entiers naturels compris entre 0 et 25 ;
- on calcule le reste y de la division euclidienne de $ax + b$ par 26 ; on détermine ainsi le plus petit entier naturel y vérifiant $y \equiv ax + b$ [26] ;
- on cherche ensuite la lettre de l'alphabet dont le rang est y ;
- cette lettre code la lettre donnée au départ.

1. Le serveur de l'entreprise utilise la clé (9 ; 15).
   a. Montrer que la lettre C est codée par la lettre H.
   b. Par quelle lettre est codée la lettre E ?
2. L'utilisateur veut décoder la lettre V associée à l'entier $y = 21$. Pour cela, il doit déterminer le plus petit entier naturel x vérifiant $21 \equiv 9x + 15$ [26].
   a. Déterminer un entier c vérifiant $9 \times c \equiv 1$ [26].
   b. Montrer que si $21 \equiv 9x + 15$ [26] alors $x \equiv 18$ [26].
   c. Décoder la lettre V.

Licence Ouverte Etalab 2.0

Exercice 10 (★★★☆)

Partie A

1. a. Décomposer le nombre 2 014 en produit de facteurs premiers.
   b. En déduire la liste des diviseurs positifs de 2 014.
2. Calculer le PGCD des nombres 2 014 et 212. On note d ce PGCD.
   Déterminer l'entier p tel que : $2\,014 = p \times d$.

Partie B

Un jury de concours doit établir l'ordre de passage des 2014 candidats qui doivent passer une épreuve orale. Le président du jury envisage la procédure automatique décrite ci-après.
Tout d'abord, il classe les 2 014 candidats par ordre alphabétique et attribue à chacun, en suivant cet ordre, un numéro allant de 1 à 2 014. Ainsi, pour définir un ordre de passage à l'oral des candidats il suffit de dresser la liste des numéros des candidats qui seront appelés l'un après l'autre à passer l'épreuve orale.
Pour établir cette liste, le président du jury choisit un entier n compris entre 1 et 400, puis procède de la manière suivante :

- le premier numéro inscrit sur la liste est le nombre n ;
- le deuxième numéro inscrit sur la liste est le nombre $2n$;
- le troisième numéro inscrit est le nombre $3n$;
- de façon générale, pour obtenir chaque numéro inscrit à partir du deuxième, on ajoute n au numéro précédent et :
  - si la somme s obtenue est inférieure ou égale à 2 014, le numéro inscrit est égal à s ;
  - sinon, le numéro inscrit est égal à $s - 2\,014$.

Par exemple, en choisissant la valeur $n = 257$, les premiers numéros inscrits sur la liste sont, dans l'ordre :

$$257 - 514 - 771 - 1\,028 - 1\,285 - 1\,542 - 1799 - 42 - 299 - 556 - \ldots - \text{ etc}$$

En effet :

- le premier numéro inscrit est $n = 257$;
- du 2e numéro (égal à 514) au 7e numéro (égal à 1 799), on a ajouté 257 au numéro précédent puisque la somme ne dépassait pas 2 014 ;
- le 8e numéro inscrit est le numéro 42 car $1\,799 + 257 = 2\,056$ et, comme 2 056 dépasse 2 014, le numéro à inscrire est $2\,056 - 2\,014 = 42$.

Ainsi le candidat 257 passera en premier l'oral ; il sera suivi du candidat 514 et ainsi de suite.
Le président du jury se demande si cette procédure permet de convoquer tous les candidats, c'est-à-dire si la liste obtenue, en 2 014 étapes, contient tous les nombres de 1 à 2 014.

1. Dans cette question, le président du jury choisit $n = 212$.
   a. Les 9 premiers numéros inscrits sont donc :
   $$212 - 424 - 636 - 848 - 1\,060 - 1\,272 - 1\,484 - 1\,696 - 1\,908.$$
   Donner la liste des 15 numéros suivants.
   La valeur $n = 212$ permet-elle de convoquer tous les candidats ?
   b. Avec cette valeur de n, combien de numéros différents la liste comporte-t-elle ?
2. Dans cette question, le président du jury choisit $n = 38$.
   Déterminer combien de numéros différents comporte la liste. Justifier la réponse. On pourra remarquer que 38 est un diviseur de 2 014.

Licence Ouverte Etalab 2.0

Exercice 11 ··· FIL ROUGE *DRONE* ··· (★☆☆☆)

Une équipe de maintenance dispose de 84 batteries et de 126 hélices. Elle souhaite préparer le plus grand nombre possible de kits **identiques**, en utilisant tout le matériel.

1. Calculer le nombre de kits préparés, puis préciser la composition d'un kit.
2. Une flotte de 72 drones doit être répartie en équipes comportant toutes le même nombre de drones, sans drone isolé. Donner la liste de toutes les tailles d'équipes possibles.
3. Un drone subit une maintenance le jeudi, puis une fois par jour pendant les jours suivants. Quel jour de la semaine sera-t-on 1 000 jours après un jeudi ?

Exercice 12 ··· UN PEU D'*INFORMATIQUE* ··· (★★☆☆)

Une entreprise répartit les requêtes entre 7 serveurs numérotés de 0 à 6 : la requête numéro n est traitée par le serveur dont le numéro est le reste de la division euclidienne de n par 7.

1. Quel serveur traite la requête numéro 2 026 ? et la requête numéro 99 999 ?
2. Montrer que les requêtes numéro n et $n + 28$ sont toujours traitées par le même serveur.
3. Déterminer le serveur qui traite la requête numéro 5^{200} (on pourra étudier les restes des premières puissances de 5 modulo 7).
4. Les numéros 1 009 et 1 011 sont-ils des nombres premiers ? Justifier.

▸ Point histoire *[Sources : Interesting Engineering, Scientific American]*

De l'Antiquité à RSA

L'arithmétique est l'une des plus anciennes branches des mathématiques : vers −300, Euclide démontre dans ses *Éléments* qu'il existe une infinité de nombres premiers et décrit l'algorithme (d'Euclide !) qui calcule le PGCD. Fermat (XVII^{e} siècle) puis Euler (XVIII^{e}) en font une théorie ; en 1801, Gauss introduit dans ses *Disquisitiones arithmeticae* les congruences et la notation ≡. Longtemps considérée comme « inutile », l'arithmétique devient au XX^{e} siècle la base de la cryptographie moderne.

En 1977, Rivest, Shamir et Adleman proposent le chiffrement **RSA** (celui de l'exercice 8) : multiplier deux grands nombres premiers est facile, mais retrouver p et q à partir de $n = pq$ est très difficile. Cette idée protège aujourd'hui les paiements en ligne ou les connexions sécurisées (`https`). Le Britannique Clifford Cocks l'avait pourtant découverte dès 1973, mais en secret, pour les services du GCHQ.

Aujourd'hui

Les clés actuelles font au moins 2 048 bits (plus de 600 chiffres). Le record de factorisation d'un nombre RSA « classique » date de 2020 (RSA-250, 829 bits), au prix de plusieurs milliers d'années de calcul cumulées. La menace vient plutôt de l'**ordinateur quantique** : l'algorithme de Shor (1994) factorise rapidement, et une étude de 2025 estime qu'il faudrait moins d'un million de *qubits* pour casser RSA-2048. Le NIST a donc publié dès 2024 des normes de cryptographie « post-quantique ».

Demain ?

L'intelligence artificielle entre aussi dans la partie : début novembre 2026, des agents d'IA de Google DeepMind ont découvert, sous supervision humaine, de nouveaux algorithmes contre RSA-1024 (une taille déjà abandonnée), mais ces résultats sont surtout théoriques et ne menacent pas les clés actuelles. Côté nombres premiers, c'est un calcul distribué sur cartes graphiques qui a découvert en 2024 le plus grand premier connu, $2^{136279841} - 1$, qui compte plus de 41 millions de chiffres !

Licence Ouverte Etalab 2.0