Exercices : Congruences

Exercice 01 ***Vrai ou Faux ?***

Entourer les congruences vraies parmi les suivantes :

1. $19 \equiv 13[6]$
2. $53 \equiv 29[5]$
3. $35 \equiv 2[11]$
4. $48 \equiv 0[12]$
5. $29 \equiv 5[6]$
6. $101 \equiv 2[7]$
7. $77 \equiv 5[12]$
8. $64 \equiv 5[9]$

Exercice 02 ***Calculs de congruences***

Compléter les congruences suivantes par le plus petit entier naturel possible :

1. $87 \equiv \ldots [7]$
2. $125 \equiv \ldots [9]$
3. $246 \equiv \ldots [11]$
4. $563 \equiv \ldots [13]$
5. $999 \equiv \ldots [8]$
6. $2025 \equiv \ldots [17]$

Exercice 03 ***Opérations sur les congruences***

1. Vérifier que $90 \equiv 6[7]$ et que $66 \equiv 3[7]$.
2. Compléter les congruences suivantes par le plus petit entier naturel possible :
   (a) $90 + 66 \equiv \ldots\ldots [7]$
   (b) $90 \times 66 \equiv \ldots\ldots [7]$
   (c) $902 \equiv \ldots\ldots [7]$
   (d) $663 \equiv \ldots\ldots [7]$
3. Faire les divisions euclidiennes de 200 et de 900 par 13 et traduire les résultats en congruences.
4. Compléter les congruences suivantes par le plus petit entier naturel possible :
   (a) $200 + 900 \equiv \ldots\ldots [13]$
   (b) $200 \times 900 \equiv \ldots\ldots [13]$
   (c) $2002 \equiv \ldots\ldots [13]$
   (d) $9003 \equiv \ldots\ldots [13]$
   (e) $2900 \equiv \ldots\ldots [13]$
   (f) $9413 \equiv \ldots\ldots [13]$

Exercice 04 ***Chiffre des unités***

Le chiffre des unités d'un nombre entier est le reste dans sa division euclidienne par 10, ou encore le résultat de ce nombre modulo 10. Par exemple, 12345 se termine par 5 et $12345 \equiv 5[10]$.

1. Quel est le chiffre des unités de $123456789 \times 987654321$?
2. Quel est le chiffre des unités de $111 \times 222 \times 333 \times 444 \times 555$?
3. ★ On cherche le chiffre des unités de 777^{2184}.
   (a) Que dit la calculatrice ?
   (b) Le nombre 2184 s'écrit $(1000\,1000\,1000)_2$ en binaire. Ainsi, $2184 = 2^{11} + 2^7 + 2^3$, et d'après les règles de calculs sur les puissances, $777^{2184} = 777^{2^{11}} \times 777^{2^7} \times 777^{2^3}$.
   Donner les valeurs de 777, 777^2, 777^{2^2}, 777^{2^3}, …, $777^{2^{11}}$. En déduire la valeur de$777^{2184}[10]$.
   (c) Conclusion ?

Exercice 05 ***Chiffrement affine***

On associe chaque lettre de l'alphabet à un nombre entre 0 et 25 (A :0 et Z :25).

Pour coder une lettre, on code son nombre associé de la manière suivante : si x est le nombre à coder, alors le nombre codé y est le reste dans la division euclidienne de $41x + 11$ par 26.

En d'autres termes : $y \equiv 41x + 11[26]$.

1. Coder le mot `ROIS`.
2. Déterminer un entier n tel que $41n \equiv 1[26]$.
3. En déduire que $x \equiv 7y - 77[26]$.
4. Décoder le mot `NPKTK`.

Exercice 06 ***Checksum***

Un protocole de transmission vérifie les données via une somme modulo 256.

On transmet les octets suivants : `[120, 34, 89, 13]`

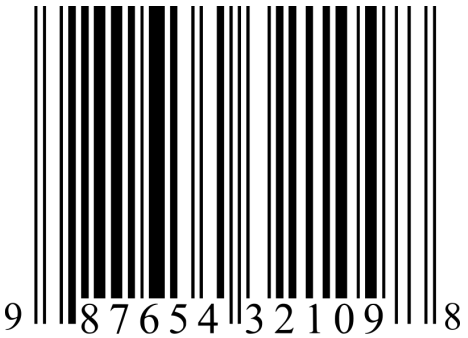
1. Calculer la somme de contrôle (*checksum*)
2. Modifier la valeur d'un octet. L'erreur est-elle détectée ?
3. Expliquer pourquoi une somme modulo n'est pas toujours fiable.

Exercice 07 ***Code barre***

Le code UPC (pour *Universal Product Code*) utilise des nombres de 12 chiffres pour désigner un produit de consommation. Les 11 premiers chiffres désignent le produit, le 12ème est une clé de contrôle destinée à détecter une erreur dans l'un des 11 premiers.

La clé de contrôle est calculée de la façon suivante :

- on calcule S_i, la somme des chiffres d'indice impair (le 1er chiffre, le 3ème, le 5ème...)
- on calcule S_p, la somme des chiffres d'indice pair (le 2ème, le 4ème, ...)
- on calcule $3 \times S_i + S_p$ modulo 10 : le résultat doit être égal à 0



1. Le code-barre ci-dessus est-il correct ?
2. Donner la clé de contrôle pour le code suivant : 0 64200 11589 _

Exercice 08 ***Code correcteur***

On considère un numéro de téléphone à 10 chiffres, auquel on ajoute 2 clés de contrôle :

- K_1 : égale à la somme des chiffres, modulo 11
- K_2 : égale à la somme pondérée par la position des chiffres, modulo 11

Par exemple, si le numéro est 07 12 34 56 78 :

- $K_1 = 0 + 7 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8[11] = 42[11] = \mathbf{10}$
- $K_2 = 0 \times 1 + 7 \times 2 + 1 \times 3 + 2 \times 4 + 3 \times 5 + 4 \times 6 + 5 \times 7 + 6 \times 8 + 7 \times 9 + 8 \times 10[11] = 290[11] = \mathbf{4}$

Le numéro est alors écrit : 07 12 34 56 78**X4** (X désignant le nombre 10).

1. Calculer les clés de contrôle du numéro suivant : 04 95 29 68 78
2. Grâce aux clés K_1 et K_2, il est possible de détecter et de corriger une éventuelle erreur qui serait commise sur un (et un seul) des chiffres du numéro.

   Détecter et corriger l'erreur dans le numéro suivant : 04 67 33 64 20 **57**

Exercice 09 ***Échange de clés***

Le **protocole de Diffie-Hellman** est une méthode cryptographique permettant à deux parties (souvent appelées Alice et Bob) de partager une clé secrète à travers un canal de communication non sécurisé.
L'idée centrale du protocole est basée sur une opération mathématique appelée **exponentiation modulaire**, et repose sur la difficulté de résoudre le logarithme discret, un problème réputé complexe en cryptographie.

Le fonctionnement est le suivant :

- Deux nombres publics sont choisis : un nombre premier p et un entier g inférieur à p, premier avec p
- Chaque participant choisit une clé privée secrète : a pour Alice et b pour Bob
- Ils calculent chacun leur clé publique : $A = g^a[p]$ pour Alice, et $B = g^b[p]$ pour Bob
- Ils s'échangent leurs clés publiques
- Chacun calcule la **même clé secrète partagée** : $K = B^a[p]$ pour Alice, et $K = A^b[p]$ pour Bob.

  En effet, $B^a = (g^b)^a = g^{ab}$ et $A^b = (g^a)^b = g^{ab}$: les clés sont bien identiques.

  Avec ce procédé, même si un attaquant voit g, p, A et B, il ne peut pas facilement trouver la clé secrète sans connaître a et b.

Pour l'exercice, considérons les paramètres publics suivants : $p = 17$ et $g = 3$.
Alice et Bob choisissent (dans le plus grand secret) leurs clés secrètes : $a = 5$ et $b = 6$.

1. Déterminer les clés publiques A et B échangées par Alice et Bob.
2. Calculer la clé secrète commune K.
3. Cette méthode est-elle infaillible ?