**Exercice 2**

**1.** Déterminer le reste dans la division euclidienne par 9 de :

**a)** $7$ ; **b)** $7^2 = 49$ ; **c)** $7^3 = 343$.

**2.** Exprimer les trois résultats précédents à l'aide de congruences.

**3.** En déduire que $7^4 \equiv 7$ (modulo 9), puis compléter et justifier les résultats suivants :

$7^5 \equiv \ldots$ (modulo 9) ; $7^6 \equiv \ldots$ (modulo 9) ;

$7^7 \equiv \ldots$ (modulo 9).

Dans la suite on admet que si $n \equiv 1$ (modulo 3), alors $7^n \equiv 7$ (modulo 9).

**4.** **a)** Démontrer que $2014 \equiv 7$ (modulo 9) et que $2014 \equiv 1$ (modulo 3).

**b)** Déduire de ce qui précède que $2014^{2014} \equiv 7$ (modulo 9).

**c)** Exprimer ce résultat par une phrase concernant le reste d'une division euclidienne à préciser.

**Exercice 3**

Un philatéliste possède 182 timbres français et 78 timbres étranger sur le foot.

Il espère vendre toute sa collection en réalisant des lots identiques, c'est-à-dire le même nombre de timbres français et étrangers.

Calculer le nombre maximum de lots qu'il pourra réaliser.

Combien y aura-t-il, dans ce cas, de timbres français et étrangers par lot ?

**Exercice 4**

Quel est le PGCD de 1065 et 852 (avec algo différence).

Quel est le PGCD de 1926 et 2996 (avec algo Euclide).

Décomposition en facteur premier de 6552.

447 est-il un nombre premier ? Expliquer pourquoi.

**Exercice 5**

Convertir en BINAIRE le nombre DECIMAL 33 (utiliserla méthode des divisions successives).

Convertir en HEXADECIMAL, le nombre BINAIRE 00111111

Calculer le nombre DECIMAL correspondant au nombre BINAIRE 101111

# Sujet A

**Exercice 1**

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 $d \times c \equiv 1 \mod K$. Le couple d'entiers $(n, d)$ est la clé privée. Alice a trouvé $d = 49$.
   Expliquer pourquoi $49 \times 9 \equiv 1 \mod 88$.

## 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 les résultats suivants :

$$2^{33} = 8589934592 \quad \text{et} \quad 8589934592 \equiv 47 \mod 115,$$

$$2^{16} = 65536 \quad \text{et} \quad 65536 \equiv 101 \mod 115.$$

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