UNIVERSITÉ DE RENNES 1

ARI – L2 – ISTIC – Université de Rennes 1

Arithmétique — Examen du 29/04/2019

Durée : 2h.
Les documents (cours, TD, ...) et les appareils (calculatrice, téléphones, ...) ne sont ***pas*** *autorisés.*
Chaque réponse devra être soigneusement justifiée *(ne pas se contenter d'une suite de calculs sans explications).*
Le barème indiqué est donné à titre indicatif.

Exercice 1. *(5 points)*

1. En utilisant l'algorithme d'Euclide, calculer le pgcd δ de 2036 et 661.
2. Déterminer un couple d'entiers $(u_0, v_0) \in \mathbb{Z}^2$ tel que $2036\,u_0 + 661\,v_0 = \delta$.
3. On considère l'équation
$$2036\,u + 661\,v = \delta \qquad (E)$$
d'inconnue $(u, v) \in \mathbb{Z}^2$. Soit (u, v) une solution de (E). Montrer qu'il existe $k \in \mathbb{Z}$ tel que $u = u_0 + 661\,k$ et $v = v_0 - 2036\,k$.
4. En déduire l'ensemble des solutions de l'équation (E).
5. Soit N un entier relatif. Déterminer l'ensemble des solutions de l'équation
$$2036\,u + 661\,v = N\,\delta \qquad (E')$$
d'inconnue $(u, v) \in \mathbb{Z}^2$.

Exercice 2. *(5 points)* On veut montrer que 1009 est un nombre premier.
Supposons le contraire.

a) Montrer que le plus petit diviseur premier de 1009 est strictement inférieur à 32.

b) Déterminer la liste des nombres premiers inférieurs à 31 ; on donnera cette liste sous la forme d'une suite croissante $p_1 \leq p_2 \leq \cdots \leq p_N$.

c) Indiquer pourquoi 1009 n'est pas divisible par 2,3, ni 5.

d) Calculer un représentant dans l'intervalle $[0, 6]$ de la classe de congruence de 100 modulo 7.

e) Pour chaque p_i, avec $i = 1, \ldots, N$, calculer un représentant dans l'intervalle $[0, p_i - 1]$ de la classe de congruence de 100 modulo p_i.

f) En écrivant $1009 = 100 \times 10 + 9$, déduire de la question précédente la classe de 1009 modulo chaque p_i.

g) Conclure.

Tournez la page

Exercice 3. *(5 points)* Pour couvrir son activité d'espionne à Bletchley Park, Alice est aussi pâtissière. Voici sa recette de pâte feuilletée. À l'étape 0, elle dispose une couche de beurre entre deux couches de pâte à pain. Ainsi, si on passait cette préparation au four, le beurre fondrait et on obtiendrait deux "feuilles de pain" l'une sur l'autre.

Pour obtenir davantage de feuilles, l'idée est simple : il suffit de replier la pâte sur elle-même et de l'étaler au rouleau afin qu'elle reprenne sa taille initiale. Ainsi, à chaque étape, Alice va replier la pâte en deux ou en trois, au choix. (Voir figure 1). Par exemple, si à l'étape 1, elle plie la pâte en trois, elle obtient trois couches de beurre, et donc, après cuisson, quatre feuilles. Si à l'étape 1 elle plie la pâte en deux, elle obtient deux couches de beurre et donc après cuisson trois feuilles. Évidemment, cette recette trahit son goût pour les messages secrets... Ici, son

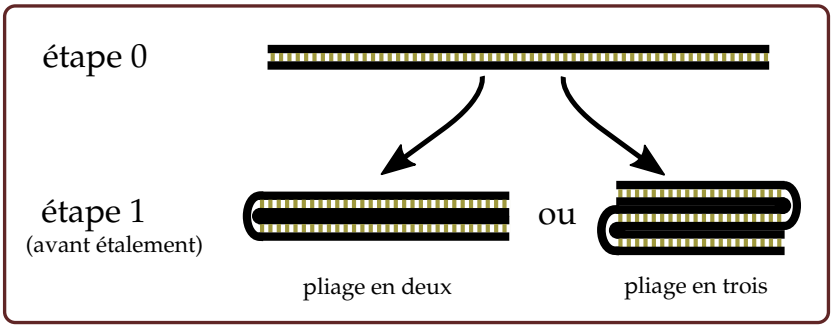

FIGURE 1 – À l'étape 1, la pâte est repliée sur elle-même en deux ou en trois, avant d'être étalée.

message secret consiste en deux nombres entiers (a, b), qu'elle va "coder" dans la recette de façon suivante : elle va plier a fois en deux et b fois en trois.

En supposant que Bob, qui reçoit la pâtisserie finale, puisse compter correctement le nombre de feuilles, on va montrer qu'il pourra retrouver les entiers a et b !

1. On note $n = a + b$ le nombre d'étapes de pliage dans la recette. Montrer *par récurrence sur* n que le nombre final de couches de beurre est $C(a, b) = 2^a 3^b$, indépendemment de l'ordre dans lequel ont été effectués les pliages.
2. Quel est le nombre final $N(a, b)$ de feuilles cuites ?
3. Expliquer comment Bob, qui ne connaît que l'entier $N = N(a, b)$, peut retrouver le code (a, b).
4. Pour célébrer la fin de la deuxième guerre mondiale, Alice fabrique avec sa recette spéciale une pâtisserie feuilletée à 1945 feuilles. Quel est le code (a, b) correspondant ?
5. Pour son anniversaire, Bob reçoit une pâtisserie à 2019 feuilles. Est-ce que cela pourrait être un message d'Alice ? (On pourra utiliser l'exercice 2, c).

Exercice 4. *(5 points)* Alice utilise le protocole RSA et publie sa clef publique $N = 221$ et $e = 5$.

1. Encoder le message $m = 15$ avec la clef publique d'Alice.
2. En fouillant dans les documents d'Alice, Charles découvre que $\varphi(N) = 192$. Avec cette information, retrouver la clef privée d'Alice.
3. Retrouver la factorisation de N à l'aide de l'information $\varphi(N) = 192$.

Fin de l'énoncé.