Exercice 1

Si n est un entier naturel strictement positif, on note $\overline{a_i a_{i-1} \dots a_1 a_0}$ son écriture décimale. On a donc $n = 10^i a_i + 10^{i-1} a_{i-1} + \dots + 10a_1 + a_0$, les entiers $a_j, 0 \leqslant j \leqslant i$, sont compris entre 0 et 9, et $a_i \neq 0$.

On désigne par q un entier compris, au sens large, entre 1 et 9, on pose $p = 10q - 1$ et l'on considère la fonction f_q qui à l'entier $n = \overline{a_i a_{i-1} \dots a_1 a_0}$ associe l'entier
$f_q(n) = \overline{a_i a_{i-1} \dots a_1} + qa_0$ (si $i = 0$, alors $f_q(n) = qa_0$).

Enfin, l'entier q étant fixé, on associe à tout entier n la suite (n_k) définie par les relations $n_0 = n$ et, pour tout entier naturel k, $n_{k+1} = f_q(n_k)$. Par exemple, si l'on fixe $q = 5$, la suite associée à 4 907 est 4 907, 525, 77, 42, 14, 21, 7, 35, 28, 42, 14,...

1. Vérifier que $f_q(n) = \dfrac{n + pa_0}{10}$. En déduire que $f_q(p) = p$.
2. (a) Montrer que, si $m > p$, alors $f_q(m) < m$.
   (b) En déduire que pour tout entier n, il existe un entier j tel que $n_j \leqslant p$.
3. (a) Montrer que, si $m < p$, alors $f_q(m) < p$.
   (b) En déduire que pour tout entier n, la suite (n_k) est périodique à partir d'un certain rang, c'est-à-dire qu'il existe des entiers k et T ($T > 0$) tels que $n_{j+T} = n_j$ pour tout $j \geqslant k$.
4. Établir que, pour tout entier n, $f_q(n)$ est congru à $q \times n$ modulo p.
5. Pour quelles valeurs de q la fonction f_q a-t-elle des points fixes (c'est-à-dire des entiers m tels que $f_q(m) = m$) autres que p ? Quels sont alors ces points fixes ?
6. Montrer que, pour des choix convenables de q, l'étude de la suite (n_k) associée à un entier n fournit des critères de divisibilité de n par 9, 19, 29, 13, 49 et 7. Énoncer ces critères.

Exercice 2

Si m_1 et m_2 sont deux entiers tels que $m_1 \leqslant m_2$, on désigne par $[\![m_1, m_2]\!]$ l'ensemble des entiers k tels que $m_1 \leqslant k \leqslant m_2$.
Si a, b et n sont trois entiers, on note $a = b$ (modulo n) lorsque a et b sont congrus modulo n, c'est-à-dire lorsque $b - a$ est multiple de n.
Dans tout cet exercice, p désigne un nombre premier.

I- Définition du logarithme discret

Pour tout $A \in \mathbb{N}$, on note $(A \bmod p)$ le reste de la division euclidienne de A par p. C'est l'unique entier de $[\![0, p-1]\!]$ congru à A modulo p.

Un entier $x \in [\![1, p-1]\!]$ est appelé une racine primitive modulo p lorsque l'ensemble des $(x^k \bmod p)$ pour $k \in \mathbb{N}$ est l'ensemble $[\![1, p-1]\!]$, c'est-à-dire lorsque les puissances de x, calculées modulo p, décrivent $[\![1, p-1]\!]$ tout entier.

1. On prend dans cette question $p = 7$. Déterminer les racines primitives modulo 7.

On admet désormais que, quel que soit le nombre premier p, il existe au moins une racine primitive modulo p. Dans la suite, on désigne par g une racine primitive modulo p.

2. (a) Montrer que l'ensemble des $(g^k \bmod p)$ pour $k \in [\![0, p-2]\!]$ est $[\![1, p-1]\!]$.
   (b) Soit $A \in [\![1, p-1]\!]$.
   Justifier l'existence et l'unicité d'un entier $a \in [\![0, p-2]\!]$ tel que $A = (g^a \bmod p)$.

a est appelé logarithme de base g modulo p de A ; on le note $\ell(A)$.

   (c) Soit b un entier naturel congru à a modulo $p - 1$. Calculer $(g^b \bmod p)$.
3. Une solution élémentaire pour déterminer $\ell(A)$ consiste à calculer les entiers $(g^k \bmod p)$, pour $k = 0, 1, \dots$, jusqu'à trouver A.
   (a) Décrire un algorithme qui réalise ce travail.
   (b) Dans cette question, on prend : $p = 53$, $A = 40$, $g = 20$ (on admettra que 20 est bien une racine primitive modulo 53).
   En programmant l'algorithme précédent sur une calculatrice, déterminer $\ell(A)$.

Exercice 3

Soit n un entier tel que $n > 6$. On considère tous les nombres $a_1, a_2, \dots, a_k$ inférieurs à n et premiers avec n et on suppose que : $a_2 - a_1 = a_3 - a_2 = \dots = a_k - a_{k-1}$ et $a_2 - a_1 > 0$.
Prouver qu'alors n est un nombre premier ou une puissance de 2.