Échanges

Codage et Cryptage

Dany-Jack Mercier
IUFM des Antilles et de la Guyane

Avec la réintroduction de l'arithmétique en terminale S, il m'a semblé opportun de présenter quelques activités sur les problèmes récents de codage et de chiffrement en portant une attention particulière au logarithme discret. Les activités décrites sont exploitables en DEUG et motivent l'apprentissage de la congruence.

1. Numéro INSEE

L'arithmétique est quotidiennement utilisée pour détecter des erreurs et protéger l'information [4]. Nous le voyons ici dans cette première activité signalée dans le fascicule de l'IREM [6] qui propose, en outre, l'étude d'autres clés de contrôle courantes telles les clés utilisées dans le numéro RIB (Relevé d'Identité Bancaire), dans le numéro I.S.B.N. (International Standard Book Number) ou encore sur le code UPC (Universal Product Code) plus connu sous le nom de code barre des supermarchés

Activité 1. Le numéro INSEE à 15 chiffres permet d'identifier chaque citoyen français. Notons-le A_1. Les 13 premiers chiffres de A_1 forment le nombre A tandis que les deux derniers chiffres constituent une clé K dont le but est de détecter quelques erreurs grossières. On peut donc écrire $A_1 = 100A + K$.
Le nombre A est obtenu de la façon suivante : en écrivant de gauche à droite, on place d'abord un 0 ou un 1 suivant qu'il s'agisse d'une femme ou d'un homme, puis les deux derniers chiffres de l'année de naissance suivis par les deux chiffres du mois de naissance. Viennent ensuite les deux chiffres du département de naissance, suivis des trois chiffres répertoriant la commune

de la naissance. Les trois derniers chiffres sont ceux de l'ordre d'inscription sur le registre d'État Civil de la commune. Enfin la clé K est égale à $97 - r$ où r désigne le reste de la division de A par 97.

1) Vérifier votre numéro INSEE.

2) On pose $A_2 = A + K$. Montrer que A_2 est divisible par 97.

3) Soient $n \in \mathbf{N}$ et $a \in \{1,2,\ldots,96\}$. Montrer que 97 ne divise jamais $a10^n$.

4) Pour vérifier la validité d'un numéro INSEE A_1, on calcule A_2. Si A_2 est divisible par 97, on estime que le numéro est valide. Sinon, on le rejette. Montrer que cette façon de procéder permet la détection d'une erreur sur un chiffre dans le numéro INSEE.

5) Montrer que l'on peut aussi détecter toute permutation de deux chiffres consécutifs dans le numéro INSEE.

6) Donner un exemple de numéro erroné non détecté par ce procédé.

Solution 1 : 2) $A_2 = A + K = 97q + r + (97 - r) \equiv 0 \ (97)$.

3) 97 est premier et les seuls facteurs premiers de $a10^n$ sont à choisir parmi les diviseurs premiers de 1, 2, …, 96. Et 97 n'est pas dans cette liste.

4) Si un seul chiffre de A_1 est modifié, il en est de même de A_2 qui devient A'_2 avec $|A'_2 - A_2| = a \cdot 10^n$ où $a \in \{1,2,\ldots,9\}$ et $n \in \mathbf{N}$. La question précédente montre que 97 ne divise pas $|A'_2 - A_2|$, donc que 97 ne divise pas A'_2, et l'erreur est détectée.

5) Supposons qu'il y ait permutation de deux chiffres consécutifs (et distincts) dans A_1. De trois choses l'une :

a) Ces deux chiffres sont dans A**.** Si l'on prime les données erronées, on a $K' = K$ et

$$|A'_2 - A_2| = |A' + K' - (A + K)| = |A' - A| = |\overline{ab} - \overline{ba}| \cdot 10^n$$

où $\overline{ab} = 10a + b$. Ainsi

$$|A'_2 - A_2| = |10a + b - (10b + a)| \cdot 10^n = 9|a - b| \cdot 10^n$$

et $9|a\text{-}b| \leq 81$ quand a et b varient dans $\{1,2,\ldots,9\}$. La question 3) montre alors que 97 ne divise pas $|A'_2 - A_2|$, donc que 97 ne divise pas A'_2, et l'erreur est détectée.

b) Ces deux chiffres sont dans K. On a $A' = A$ et $|A'_2 - A_2| = |K' - K|$ de sorte que le raisonnement est le même que le précédent.

c) Ces deux chiffres sont l'un dans A*, l'autre dans* K. Il existe un entier naturel B tel que

$$\begin{cases} A_2 = A + K & \text{où } A_1 = B\cdot 10^3 + a\cdot 10^2 + b\cdot 10 + c \\ A'_2 = A' + K' & \text{où } A'_1 = B\cdot 10^3 + b\cdot 10^2 + a\cdot 10 + c \end{cases}$$

Donc A = 10B + a, K = 10b + c, A′ = 10B + b, K′ = 10a + c, et

$$|A'_2 - A_2| = 9|a-b|\cdot 10^n .$$

On conclut comme en a).

6) On additionne 97 à un vrai numéro INSEE.

2. Chiffrement affine

Abordons maintenant le domaine important de la cryptographie et de la protection des données. Le chiffrement proposé ici (et cité en [6]) n'est pas suffisant, mais permet une incursion dans les problèmes spécifiques à la cryptographie : création de clés de chiffrement, fonctions « sens unique » et méthode d'attaque contre un message crypté.

Activité 2. Soit I = {0,1,2…,25}. Représentons chaque lettre de l'alphabet par un élément de l'anneau **Z**/26**Z** ou, ce qui revient au même, par un nombre de I. On se propose de chiffrer un message en utilisant une clé $(a,b) \in I^2$ et en procédant de la façon suivante : à tout $\dot{x} \in \mathbf{Z}/26\mathbf{Z}$, on associe l'élément $f_{(a,b)}(\dot{x}) = a\dot{x} + \dot{b}$ définissant ainsi une application $f_{(a,b)}$: **Z**/26**Z** → **Z**/26**Z**. Pour que cette application représente bien une fonction de chiffrement, il faut et il suffit qu'elle soit injective.

1) Montrer l'équivalence entre
   i) $f_{(a,b)}$ est injective,
   ii) $f_{(a,b)}$ est surjective,
   iii) a est premier avec 26.

2) Déterminer l'ensemble $(\mathbf{Z}/26\mathbf{Z})^*$ de tous les éléments $\dot{a}$ de **Z**/26**Z** tels que a soit premier avec 26.

3) Montrer que $(a_1,b_1) \neq (a_2,b_2)$ entraîne $f_{(a_1,b_1)} \neq f_{(a_2,b_2)}$. En déduire le nombre de clés (a,b) possibles.

4) On suppose ici que $(a,b) = (17,3)$.
   a) Trouver une solution de l'équation $17x - 26k = 1$ dans **Z**.
   b) Pour $\dot{y} \in \mathbf{Z}/26\mathbf{Z}$, exprimer $f^{-1}_{(17,3)}(\dot{y})$ en fonction de $\dot{y}$ et montrer l'existence d'un couple (a',b') tel que $f^{-1}_{(17,3)} = f_{(a',b')}$. La fonction $f^{-1}_{(17,3)}$ permet de déchiffrer le message.

5) Le but de cette question est de montrer la faiblesse du chiffrement affine devant une attaque : si g désigne la fonction réciproque de $f_{(a,b)}$, montrer que $g(\dot{y}) = \dot{a}'\left(\dot{y} - \dot{b}\right)$ pour un $\dot{a}'$ convenable, puis expliquer comment s'organiser pour trouver la clé de déchiffrement

6) Une autre attaque peut être menée de la façon suivante. On peut calculer la fréquence d'apparition des symboles dans le message chiffré, puis avoir une idée de la traduction de certaines lettres. À partir de ces données probables, on déchiffre entièrement le message pour voir s'il ne devient pas clair. On recommence ce procédé jusqu'à l'obtention du message en clair. Voyons ce que ceci donne dans la pratique…

Supposons connues les traductions de $\dot{20}$ et $\dot{23}$. Pouvez-vous trouver la clé (a,b) du chiffrement affine tel que $f_{(a,b)}(\dot{5}) = \dot{20}$ et $f_{(a,b)}(\dot{10}) = \dot{23}$?

Solution 2 : 1) $f_{(a,b)}$: $\mathbf{Z}/26\mathbf{Z} \to \mathbf{Z}/26\mathbf{Z}$ est injective si, et seulement si, $f_{(a,b)}(\mathbf{Z}/26\mathbf{Z})$ est équipotent à l'ensemble de départ, i.e. de cardinal 26. Compte tenu de l'inclusion $f_{(a,b)}(\mathbf{Z}/26\mathbf{Z}) \subset \mathbf{Z}/26\mathbf{Z}$, ceci équivaut à l'égalité $f_{(a,b)}(\mathbf{Z}/26\mathbf{Z}) = \mathbf{Z}/26\mathbf{Z}$, soit à la surjectivité de $f_{(a,b)}$. On a montré l'équivalence entre i) et ii).L'équivalence entre ii) et iii) provient des équivalences :

$$f_{(a,b)} \text{ surjective} \Leftrightarrow \forall \dot{y} \in \mathbf{Z}/26\mathbf{Z}\ \exists \dot{x} \in \mathbf{Z}/26\mathbf{Z}\ \exists k \in \mathbf{Z} \quad ax + b = y + 26k$$
$$\Leftrightarrow \forall y \in \mathbf{Z}\ \exists x, k \in \mathbf{Z} \quad ax - 26k = y - b$$
$$\Leftrightarrow \exists x, k \in \mathbf{Z} \quad ax - 26k = 1 \Leftrightarrow \text{pgcd}(a, 26) = 1$$

2) L'image de 26 par la fonction indicatrice d'Euler est $\varphi(26) = (2-1)(13-1) = 12$. Il y aura donc 12 éléments dans $(\mathbf{Z}/26\mathbf{Z})^*$. On trouve $(\mathbf{Z}/26\mathbf{Z})^* = \{1,3,5,7,9,11,15,17,19,21,23,25\}$

3) Si $f_{(a_1,b_1)} = f_{(a_2,b_2)}$, alors, en particulier, les images de $\dot{0}$ et de $\dot{1}$ coïncident, i.e. $\dot{b}_1 = \dot{b}_2$ et $\dot{a}_1 + \dot{b}_1 = \dot{a}_2 + \dot{b}_2$. Ceci entraîne $(\dot{a}_1, \dot{b}_1) = (\dot{a}_2, \dot{b}_2)$, soit $(a_1,b_1) = (a_2,b_2)$. Il y aura 12 choix possibles pour a, puis 26 choix possibles pour b, ce qui nous fera $12 \times 26 = 312$ clés au total.

4.a) L'algorithme d'Euclide s'écrit

$$26 = 17 \times 1 + 9\ ;\ 17 = 9 \times 1 + 8\ ;\ 9 = 8 \times 1 + 1,$$

d'où, après calculs, $17(-3) - 26(-2) = 1$.

4.b) Pour $\dot{y}$ donné, il faut résoudre l'équation $f_{(17,3)}(\dot{x}) = 17\dot{x} + \dot{3} = \dot{y}$ en $\dot{x}$.

Première solution : Cherchons les entiers x, k vérifiant $17x - 26k = y - 3$.

$$17x-26k=y-3 \Leftrightarrow \begin{cases}17x-26k=y-3\\17(-3)(y-3)-26(-2)(y-3)=y-3\end{cases}$$
$$\Leftrightarrow 17(x+3y-9)=26(k+2y-6) \qquad (*)$$

17 divise $26(k+2y-6)$ en étant premier avec 26, donc divise $(k+2y-6)$ et il existera un entier u tel que $k+2y-6=17u$. En remplaçant dans (*), on obtient

$$\begin{cases}x=9-3y+17u\\k=6-2y+17u\end{cases} \text{ où } u\in\mathbf{Z}.$$

Ainsi $f^{-1}_{(17,3)}(\dot{y})=\dot{9}-3\dot{y}=\dot{9}+23\dot{y}=f_{(23,9)}(\dot{y})$.

Deuxième solution : On anticipe sur la question 5. Chercher l'inverse de $\dot{17}$ revient à résoudre $17x-26k=1$ dans $\mathbf{Z}$. On trouve $\dot{17}^{-1}=-\dot{3}$, donc

$$17\dot{x}+\dot{3}=\dot{y}\Leftrightarrow \dot{x}=-\dot{3}(\dot{y}-\dot{3})=23\dot{y}+\dot{9}.$$

5) Par hypothèse, $\dot{a}$ est inversible dans $\mathbf{Z}/26\mathbf{Z}$, donc

$$f_{(a,b)}(\dot{x})=a\dot{x}+\dot{b}=\dot{y}\Leftrightarrow \dot{x}=\dot{a}'(\dot{y}-\dot{b}) \quad (**)$$

Ainsi $g(\dot{y})=\dot{a}'(\dot{y}-\dot{b})$ où $\dot{a}'$ est l'inverse de $\dot{a}$. Il suffit de faire décrire l'ensemble $(\mathrm{Z}/26\mathrm{Z})^*\times \mathrm{Z}/26\mathrm{Z}$ à $(\dot{a}',\dot{b})$, i.e. d'envisager $12\times 26=312$ possibilités, pour trouver la clé de déchiffrement. Remarquons au passage que (**) prouve que la fonction g de déchiffrement associée à $f_{(a,b)}$ est de la forme $f_{(a',b')}$ et que $f^{-1}_{(a,b)}(\dot{y})=\dot{a}'\dot{y}-\dot{a}'\dot{b}=f_{(c,d)}(\dot{y})$ où $(c,d)=(a' \bmod 26, a'b \bmod 26)$ (ici $e \bmod 26$ représente le reste de la division euclidienne de e par 26).

6)

$$\begin{cases}f_{(a,b)}(\dot{5})=\dot{20}\\f_{(a,b)}(\dot{10})=\dot{23}\end{cases}\Leftrightarrow\begin{cases}a\dot{5}+\dot{b}=\dot{20}\\a\dot{10}+\dot{b}=\dot{23}\end{cases}\Rightarrow 5\dot{a}=\dot{3}$$

Comme $\dot{5}\times(-\dot{5})=\dot{1}$, l'inverse de $\dot{5}$ sera $-\dot{5}=\dot{21}$. L'équation $5\dot{a}=\dot{3}$ équivaut donc à $\dot{a}=(-\dot{5})\dot{3}=\dot{11}$, d'où $\dot{b}=\dot{20}-5\dot{a}=\dot{20}-\dot{3}=\dot{17}$.

3. Cryptosystème utilisant l'exponentiation

Les paragraphes 3.1 à 3.4 sont traités dans le cadre général d'un corps fini $\mathbf{F}_q$ à $q=p^s$ éléments (où p est un nombre premier et $s\in\mathbf{N}^*$) et font référence à [2]. Ils permettent de nous placer dans le contexte du paragraphe 3.5 dont les

activités seront de niveau terminale ou DEUG et n'utiliseront que des congruences modulo p.

3.1. Logarithme discret

Le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique. On peut donc trouver un élément b qui engendre multiplicativement $\mathbf{F}_q^*$, i.e. tel que $\mathbf{F}_q^* = \{1,b,b^2,\ldots,b^{q-2}\}$. Un tel élément b est appelé élément primitif de $\mathbf{F}_q$. L'application de $\{0,1,\ldots,q-2\}$ qui à r associe b^r est une bijection d'inverse notée ind_b et appelée logarithme discret en base b, ou encore index en base b. Ainsi :

$$0 \le r \le q-2 \text{ et } x = b^r \Leftrightarrow r = \mathrm{ind}_b(x).$$

Puisque b est d'ordre $q-1$,

$$\begin{aligned} b^{\mathrm{ind}_b(xy)} = b^{\mathrm{ind}_b(x)} \cdot b^{\mathrm{ind}_b(y)} &\Leftrightarrow b^{\mathrm{ind}_b(xy)-\mathrm{ind}_b(x)-\mathrm{ind}_b(y)} = 1 \\ &\Leftrightarrow (q-1) \mid (\mathrm{ind}_b(x) - \mathrm{ind}_b(x) - \mathrm{ind}_b(y)) \\ &\Leftrightarrow \mathrm{ind}_b(xy) \equiv \mathrm{ind}_b(x) + \mathrm{ind}_b(y) \quad (q-1) \end{aligned}$$

et l'on retrouve la relation caractéristique des fonctions logarithmes. En d'autre termes, la fonction ind_b définie sur $(\mathbf{F}_q^*,\cdot)$ et à valeurs dans le groupe additif $\mathbf{Z}/(q-1)\mathbf{Z}$ est un homomorphisme de groupes.

Le problème du calcul explicite de l'index d'un élément quelconque de $\mathbf{F}_q^*$ est connu sous le nom de problème du logarithme discret. C'est un problème dont la complexité croît rapidement avec q si bien que l'on puisse estimer que, pour $q > 2^{100}$, l'exponentiation $r \mapsto b^r$ constitue une fonction trappe (ou fonction à sens unique). Ceci signifie que le calcul de b^r à partir de r s'effectue en un temps raisonnable, mais que, réciproquement, l'obtention de l'index de $y \in \mathbf{F}_q^*$ est impossible en un temps satisfaisant. C'est cette propriété qui nous permet de construire un cryptosystème basé sur l'exponentiation dans le paragraphe suivant.

3.2 Principe du chiffrement

Tout élément x de $\mathbf{F}_q^*$ vérifie l'égalité fondamentale $x^{q-1} = 1$. Si a désigne un entier tel que $1 \le a \le q-2$ et $\mathrm{pgcd}(a,q-1) = 1$, le théorème de Bezout assure de l'existence de deux entiers u et v tels que $au + (q-1)v = 1$, de sorte que

$$x = x^{au+(q-1)v} = x^{au} \quad (*)$$

pour tout $x \in \mathbf{F}_q^*$. Supposons que $x \in \mathbf{F}_q^*$ soit le message à transmettre. Le message chiffré sera $f(x) = x^a$ tandis que le déchiffrement se fera à l'aide de la fonction $g(y) = y^u$, pour retrouver

$$g(f(x)) = g(x^a) = x^{au} = x.$$

Les fonctions d'exponentiation f et g sont faciles à mettre en œuvre et, cependant, l'attaque d'un tel cryptosytème demeure difficile dès que q est assez grand. En effet, un pirate qui possèderait à la fois un message en clair x et le message chiffré $y = x^a$ serait dans l'impossibilité de trouver la clé a, tout simplement parce que la résolution de l'équation $y = x^a$ en a équivaut à la résolution de l'équation

$$a \operatorname{ind}_b(x) \equiv \operatorname{ind}_b(y) \quad (q - 1)$$

et suppose que l'on sache résoudre le problème du logarithme discret. Un algorithme qui fonctionne bien dès que $q-1$ se factorise en utilisant seulement de « petits » nombres premiers est détaillé au paragraphe suivant.

Notons que la nature du cryptosystème que nous venons de décrire est identique à celle du procédé R.S.A. détaillé en [3]. Il suffit de remplacer $\mathbf{F}_q$ par $\mathbf{Z}/n\mathbf{Z}$ où $n = pq$ est le produit de deux entiers premiers très grands. Ici $\mathbf{Z}/n\mathbf{Z}$ n'est plus un corps, mais on peut toujours travailler dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$. Ce groupe est d'ordre $\varphi(n) = (p-1)(q-1)$. Pour un entier a premier avec $\varphi(n)$, on obtient une équation du style $au + \varphi(n)v = 1$ et l'analogue de la relation (*), à savoir $x = x^{au}$ pour tout $x \in (\mathbf{Z}/n\mathbf{Z})^*$.

3.3. Algorithme de Silver-Pohlig-Hellmann

Le but de cet algorithme est le calcul de l'index $r = \operatorname{ind}_b(x)$ où $x \in \mathbf{F}_q^*$ et où b est un élément primitif de $\mathbf{F}_q$. Il faut trouver r tel que $x = b^r$. Soit $q-1 = \prod_{i=1}^{m} p_i^{\alpha_i}$ la décomposition en produits de facteurs premiers de $q-1$. Pour $i \in \mathbf{N}_m$, écrivons :

$$r \equiv r_0 + r_1 p_1 + \ldots + r_{\alpha_i - 1} p_i^{\alpha_i - 1} \qquad (p_i^{\alpha_i})$$

avec $r_j \in \{0,\ldots,p_i-1\}$.

On a $x^{\frac{q-1}{p_i}} = \left(b^{\frac{q-1}{p_i}} \right)^{r_0}$ et, comme $b^{\frac{q-1}{p_i}}$ est une racine p_i-ème primitive de l'unité, cette équation détermine parfaitement r_0. On recommence ensuite de la même façon en prenant soin de remplacer x par xb^{-r_0} et la puissance $\frac{q-1}{p_i}$ par $\frac{q-1}{p_i^2}$:

$$\left(xb^{-r_0}\right)^{\frac{q-1}{p_i^2}} = \left(b^{r-r_0}\right)^{\frac{q-1}{p_i^2}} = \left(b^{\frac{q-1}{p_i}}\right)^{r_1}.$$

Ici encore, cette équation détermine entièrement r_1, et ainsi de suite. Au bout du compte on connaît les entiers l_i tels que $r \equiv l_i \quad (p_i^{\alpha_i})$ et le théorème Chinois permettra de calculer r modulo $q-1$. Cet algorithme sera utilisé dans l'activité 7 plus bas.

3.4. Autre application : échange de clés sur un réseau

Une autre utilisation importante de l'exponentiation dans un corps fini est l'échange de clés secrètes. Cet échange est pratiqué lorsqu'on envisage par la suite d'utiliser un cryptosystème conventionnel tel le D.E.S. (Digital Encryption Standard) : la fonction de chiffrage et celle de déchiffrage sont alors entièrement commandées par la connaissance d'une clé unique K qui doit demeurer secrète. Le choix et la transmission de cette clé ne sont pas une chose aisée pour nos deux interlocuteurs A et B qui viennent de faire connaissance sur le réseau. Bien sûr, nos deux interlocuteurs auraient pu utiliser un cryptosystème à clés révélées comme le système R.S.A. ([3]), mais ceci nécessite d'être inscrit sur un bottin public. On peut aussi objecter que les systèmes à clés révélées sont plus lents que leurs homologues conventionnels. Et c'est bien ce qui se passe dans la pratique : en l'état actuel, les systèmes à clés publiques sont principalement utilisés pour la distribution de clés nécessaires au fonctionnement de cryptosystèmes conventionnels.
Décrivons le schéma de Diffie-Hellmann ([2]). Supposons que deux personnes A et B désirent utiliser un réseau informatique pour s'échanger une clé secrète. A choisit un entier h dans $\{2,3,\ldots,q-2\}$ et transmet b et b^h à B en utilisant le réseau. B fait de même en choisissant un entier k dans $\{2,3,\ldots,q-2\}$, puis en expédiant b^k en clair à A. Il ne reste qu'à choisir $K = b^{hk}$ comme clé commune et secrète. En effet, A peut calculer $(b^k)^h = K$ et B calcule $(b^h)^k = K$. Si les nombres b, b^h et b^k ont circulé sur le réseau, ils ne suffisent pas à découvrir la clé b^{hk} puisque le calcul de b^{hk} à partir b^h et b^k est encore un problème non résolu, même si l'on connaît b.

3.5. Activités

Activité 3 (Petit Théorème de Fermat)
Soient p un nombre premier et a un entier relatif quelconque. Montrer que

l'entier $(a + 1)^p - a^p - 1$ est divisible par p. En déduire que $a^p - a$ est divisible par p.

Solution 3 : On a $(a+1)^p - a^p - 1 = \sum_{k=1}^{p-1} C_p^k a^k$ par la formule du binôme de Newton et l'on montre que p divise C_p^k pour tout $k \in \{1,\ldots,p-1\}$. En effet, $p! = k!(p-k)!C_p^k$ montre que p divise $k!(p-k)!C_p^k$. L'entier p, premier, sera premier avec tout nombre qu'il ne divise pas. En particulier p sera premier avec k, $k-1$, etc, donc sera premier avec le produit k!(p-k)!. Le théorème de Gauss montre alors que p divise C_p^k.

Montrons que $a^p - a$ est divisible par p par récurrence sur a (lorsque $a \in \mathbf{N}$). C'est trivial si $a = 0$. Si c'est vrai au rang a,

$$(a+1)^p - (a+1) = [(a+1)^p - a^p - 1] + [a^p - a].$$

L'hypothèse récurrente montre que p divise les deux termes entre crochets, donc divise $(a + 1)^p - (a + 1)$ et la propriété sera héréditaire. Si $a < 0$, on peut toujours écrire la division euclidienne $a = pq + r$ avec $0 \leq r < p$ (si l'on veut éviter les congruences) et développer l'expression $(a + 1)^p - (a + 1)$ pour ramener le problème à la divisibilité de $(r + 1)^p - (r + 1)$ déjà résolu.

Activité 4 (Ordre multiplicatif d'un élément de $\mathbf{F}_p$)

Soit p un nombre premier. Notons $\mathbf{F}_p$ l'anneau $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{F}_q^* = \mathbf{F}_p \backslash \{0\}$.

1) Montrer que, pour tout élément x de $\mathbf{F}_q^*$, il existe $x' \in \mathbf{F}_q^*$ tel que $x \cdot x' = 1$. En utilisant le petit théorème de Fermat, déduire que $x^{p-1} = 1$ pour tout $x \in \mathbf{F}_q^*$.

2) Soit $x \in \mathbf{F}_q^*$. Montrer qu'il existe un plus petit entier naturel non nul e vérifiant $x^e = 1$. e s'appelle l'ordre multiplicatif de x. Montrer ensuite, en utilisant une division euclidienne, que :

a) $x^k = 1 \Leftrightarrow e \mid k$,

b) L'ensemble Λ_x des puissances de x possède e éléments et

$$\Lambda_x = \{1, x, x^2, \ldots, x^{e-1}\}.$$

Solution 4 : 1) Si $x = \dot{\eta}$ avec $\eta \in \{1,\ldots,p-1\}$, le théorème de Bezout montre l'existence de deux entiers u, v tels que $\eta u + pv = 1$, d'où $\dot{\eta}\dot{u} = 1$ et il suffit de prendre $x' = \dot{u}$. L'activité précédente entraîne $x^p = x$, d'où l'identité demandée en multipliant les deux membres par x'.

2) Comme $x^{p-1} = 1$, l'ensemble des entiers naturels non nuls k vérifiant $x^k = 1$ n'est pas vide. Étant inclus dans $\mathbf{N}$, il possèdera un plus petit élément e.

Montrons a) : Si $k = eq$, alors $x^k = (x^e)^q = 1$. Réciproquement, si $x^k = 1$, la division euclidienne de k par e s'écrit $k = eq + r$ avec $0 \leq r < e$. On déduit $x^k = x^r = 1$, d'où $r = 0$ pour ne pas contradire la définition de e.
Montrons b) : La division euclidienne ci-dessus montre immédiatement que $\Lambda_x = \{1,x,x^2,\ldots,x^{e-1}\}$. Il suffit de vérifier que deux éléments x^t et x^s où $0 \leq t$, $s < e$ ne sont jamais égaux pour conclure à $\#\Lambda_x = e$. L'égalité $x^t = x^s$ entraîne $x^{t-s} = 1$ avec, par exemple, $t \geq s$. D'après a), ceci implique que e divise $t-s$, et, comme $0 \leq t-s < e$, ceci entraîne $t = s$.

Activité 5 (Puissances d'un élément dans $\mathbf{F}_{127}$)

1) Montrer que 127 est un nombre premier.
2) Écrire un programme permettant de calculer l'ordre e d'un élément x de $\mathbf{F}_{127}^*$ (i.e. de trouver le plus petit entier naturel non nul e vérifiant $x^e = 1$). En déduire que $\mathbf{F}_{127}^* = \{1,3,3^2,\ldots,3^{125}\}$ en utilisant l'activité 4.

3) De façon indépendante de ce qui précède, voici une méthode permettant de calculer une puissance de 3 dans $\mathbf{F}_{127}^*$, par exemple 3^{73}.

a) Calculer d'abord les nombres 3, 3^2, 3^{2^2}, 3^{2^3}, 3^{2^4}, 3^{2^5}, 3^{2^6} dans $\mathbf{F}_{127}^*$.
b) Exprimer 73 en base 2, puis en déduire 3^{73}.

Solution 5 : 1) C'est l'occasion d'utiliser le crible d'Érathostène. 127 n'est pas divisible par 2, 3, 5, 7, 11, 13 et $13^2 > 127$, donc on peut s'arrêter.

2) En basic :

```
10 INPUT A : B = A : I = 1
15 IF A<=1 OR A>=127 THEN 10
20 I = I+1 : B = B*A
30 IF B>126 THEN B = B-INT(B/127)*127
40 IF B = 1 THEN PRINT ''L'ordre de''; A ;''est''; I : END
50 GOTO 20
```

Un tel programme montre que l'ordre multiplicatif de 3 est 126, autrement dit que l'ensemble Λ_3 des puissances de 3 possède 126 éléments et que $\Lambda_3 = \{1,3,3^2,\ldots,3^{126}\}$. Comme $\mathbf{F}_{127}^*$ possède 126 éléments, on aura $\mathbf{F}_{127}^* = \Lambda_3$.

3.a) Dans $\mathbf{F}_{127}$, $3^2 = 9$, donc $3^{2^2} = (3^2)^2 = 81$, puis

$$3^{2^3} = (3^{2^2})^2 = 81 = 84 \pmod{127}$$

et ainsi de suite pour obtenir :

1	3	3^2	3^{2^2}	3^{2^3}	3^{2^4}	3^{2^5}	3^{2^6}
1	3	9	81	84	71	88	124 = -3

3.b) $73 = 2^6 + 2^3 + 1$, donc

$$3^{73} = 3^{2^6} \times 3^{2^3} \times 3^1 = -3 \times 84 \times 3 = -756 = 6 \pmod{127}.$$

Activité 6 (Cryptosystème utilisant l'exponentiation dans $\mathbf{F}_{127}$)

Le tableau ci-dessous permet d'associer un nombre de $\mathbf{F}_{127}^*$ à chacune des lettres de l'alphabet et à quelques signes de ponctuation. Par exemple la lettre H est représentée par le chiffre 8. En fait on représentera au hasard la lettre H par 8, 38, 68 ou 98 pour éviter que l'on casse trop facilement ce cryptosystème en calculant la fréquence d'apparition des symboles dans un message chiffré. Avec cette convention, 54 représente aussi la lettre X.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	.	,	‘	espace
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

5 et 126 sont premiers entre eux et l'algorithme d'Euclide permet d'obtenir l'identité $101 \times 5 - 4 \times 126 = 1$. Le théorème de Fermat montre que $x^{126} = 1$, d'où $x = x^{101\times5-4\times126} = x^{101\times5}$ pour tout $x \in \mathbf{F}_{127}^*$. Si l'on pose $f(x) = x^5$ et $g(y) = y^{101}$, on aura $g \circ f(x) = x$. Ceci nous invite à choisir f comme fonction de chiffrement et g comme fonction de déchiffrement. Prenons par exemple le message SALUT. On le traduit en chiffres de $\mathbf{F}_{127}^*$ grâce au tableau ci-dessus, ce qui donne (par exemple) 19-1-42-81-20. On applique la clé de chiffrement f pour obtenir :

$f(19)–f(1)–f(42)–f(81)–f(20) = 19^5–1^5–42^5–81^5–20^5 = 107–1–104–36–108.$

Le message chiffré est 107–1–104–36–108. Pour le déchiffrer, on calculera chacune des images de ces nombres par g.

1) Écrire un programme permettant le calcul de la puissance n-ième d'un élément x de $\mathbf{F}_{127}^*$.

2) Déchiffrer le message

124–35–9–74–31–111–82–116–2–121–79–29–62–83–107.

Solution 6 : 1) Par exemple en basic et en utilisant la fonction partie entière INT,

```
1 REM Calcul de X puissance N dans F127
5 PRINT ''X PUISSANCE N''
10 INPUT ''X =''; X ,''N =''; N : Y=1
15 IF X<=0 OR X>=127 THEN 10
20 FOR I=1 TO N : Y = Y*X
```

```
25 IF Y>126 THEN Y = Y-INT(Y/127)*127
30 NEXT I
35 PRINT X ; ''PUISSANCE''; N ;''=''; Y
40 END
```

2) $g(124) = 124^{101} = 17$ correspond à la lettre Q… Le message en clair sera après calculs « QUE DE CHIFFRES ».

Activité 7 (Attaque du cryptosystème de l'activité 6)

Un pirate vient d'avoir accès à un message en clair et à son chiffrage. Il sait aussi que la méthode de chiffrement employée est celle de l'exponentiation dans $\mathbf{F}_{127}$ décrite dans l'activité 6. Le message en clair est 20 tandis que le message chiffré est 108. Il se propose de déterminer des clés possibles a du chiffrement, puis de rechercher la clé u de déchiffrement. Il s'agit donc dans un premier temps de trouver l'entier a de $\{0,1,\ldots,125\}$ vérifiant $20^a = 108$ dans $\mathbf{F}_{127}$. On a vu dans l'activité 5 que l'ordre multiplicatif de 3 est 126, autrement dit que $\mathbf{F}_{127}^* = \{1,3,3^2,\ldots,3^{125}\}$. La bijection qui, à $x \in \mathbf{F}_{127}^*$, associe $r \in \{0,1,\ldots,125\}$ tel que $x = 3^r$ s'appelle « le logarithme discret en base 3 » ou « index en base 3 » et l'on note $r = \mathrm{ind}_3(x)$.

1) Montrer que pour tout $x, y \in \mathbf{F}_{127}^*$,

$$\mathrm{ind}_3(xy) \equiv \mathrm{ind}_3(x) + \mathrm{ind}_3(y) \quad (126)$$

et en déduire que $\mathrm{ind}_3(x^n) \equiv n\,\mathrm{ind}_3(x)$ (126) pour tout $n \in \mathbf{N}$.

2) Montrer que l'équation $20^a = 108$ dans $\mathbf{F}_{127}^*$ équivaut à la congruence :

$$a\,\mathrm{ind}_3(20) \equiv \mathrm{ind}_3(108)\ (126).$$

3) Cette question propose une méthode de calcul de l'index $r = \mathrm{ind}_3(20)$ connue sous le nom d'algorithme de Silver-Pohlig-Hellman. On a $20^r = 1$ et $126 = 2\cdot 3^2\cdot 7$.

a) Si $r \equiv r_0$ (2) avec $r_0 \in \{0,1\}$, vérifier que $20^{63} = 3^{63r_0}$. En déduire $r_0 = 1$.

b) Si $r \equiv s_0 + s_1\cdot 3$ (3^2) avec $s_0, s_1 \in \{0,1,2\}$, montrer que $20^{42} = 3^{42s_0}$, puis en déduire $s_0 = 0$. Montrer ensuite que $20^{14} = 3^{42s_1}$. En déduire $s_1 = 2$.

c) Si $r \equiv t_0$ (7) avec $t_0 \in \{0,\ldots,6\}$, vérifier que $20^{18} = 3^{18t_0}$. En déduire $t_0 = 0$.

d) Trouver l'unique nombre r de $\{0,1,\ldots,125\}$ satisfaisant les trois conditions $r \equiv 1$ (2), $r \equiv 6$ (9) et $r \equiv 0$ (7).

4) On admet que $\mathrm{ind}_3(108) = 21$. Trouver tous les éléments a de $\mathbf{F}_{127}^*$ satisfaisant l'équation $20^a = 108$. Dites bièvement comment on pourrait déterminer la clé a utilisée dans le chiffrement.

Solution 7 : 1) Comme 3 est d'ordre 126, l'égalité

$$3^{\mathrm{ind}_3(xy)} = 3^{\mathrm{ind}_3(x)} \cdot 3^{\mathrm{ind}_3(y)}$$

équivaut à la divisibilité de $(\mathrm{ind}_3(xy) - \mathrm{ind}_3(x) - \mathrm{ind}_3(y))$ par 126. La seconde identité se montre par récurrence sur n.

2) $20^a = 108$ équivaut à $3^{a\,\mathrm{ind}_3(20)} = 3^{a\,\mathrm{ind}_3(108)}$ ou encore à :

$$a\,\mathrm{ind}_3(20) \equiv \mathrm{ind}_3(108)\ (126)$$

puisque 3 est d'ordre multiplicatif 126.

3a) On a $20^{\frac{126}{2}} = 3^{\frac{126}{2}r_0}$, soit $20^{63} = 3^{63r_0}$ puisque $3^{126} = 1$.
Ceci entraîne $-1 = (-1)^{r_0}$, d'où $r_0 = 1$.

3b) De même

$$20^{\frac{126}{3}} = 3^{\frac{126}{3}(s_0+3s_1)} \Leftrightarrow 20^{42} = 3^{42s_0} \Leftrightarrow 1 = 107^{s_0} \Leftrightarrow s_0 = 1$$

et

$$20^{\frac{126}{3^2}} = 3^{\frac{126}{3^2}(s_0+3s_1)} \Leftrightarrow 20^{14} = 3^{\frac{126}{3}s_1} \Leftrightarrow 19 = 107^{s_1}.$$

Puisque $107 = 3^{\frac{126}{3}}$ est une racine primitive 3-ème de l'unité, s_1 s'en déduit. On trouve $107^2 = 19$, donc $s_1 = 2$.

3c)

$$20^{\frac{126}{7}} = 3^{\frac{126}{7}r} \Leftrightarrow 20^{18} = 3^{\frac{126}{7}t_0} \Leftrightarrow 1 = 4^{t_0} \Leftrightarrow t_0 = 0.$$

3d) On résout le système (cf. [1] ou [5]) :

$$\begin{cases} r = 1 + 2u \\ r = 7v \\ r = 6 + 9w \end{cases} \qquad \text{avec } u, v, w \in \mathbf{Z}$$

pour trouver $r = 105$, soit $\mathrm{ind}_3(20) = 105$.

4)
$20^a = 108 \Leftrightarrow a\,\mathrm{ind}_3(20) \equiv \mathrm{ind}_3(108)\ (126) \Leftrightarrow 105a \equiv 21\ (126) \Leftrightarrow 5a \equiv 1\ (6)$
Cette dernière congruence équivaut à $a \equiv 5\ (6)$. On obtient toute une série de clés probables ayant permis le chiffrement, à savoir les nombres $a = 5 + 6k$ où $k \in \mathbf{Z}$. Pour chacun de ces nombres a, on détermine $u \in \{0,\ldots,126\}$ tel qu'il existe $v \in \mathbf{Z}$ avec $au + 126v = 1$, puis on teste la clé $g(y) = y^u$ de déchiffrement possible sur le reste du message pour voir s'il ne devient pas lisible. Une autre méthode consisterait à recommencer la recherche de conditions sur a en utilisant une autre lettre chiffrée dont on connaîtrait la traduction.

Références

[1] Itard J., « Arithmétique et théorie des nombres », PUF, collection Que sais-je ?, n° 1093, 1963.
[2] Lidl R. & Niederreiter H., « Introduction to finite fields and their applications », Cambridge Univ. Press, 1988.
[3] Mercier D.-J., « Cryptographie classique et cryptographie publique à clé révélée », A.P.M.E.P., Bulletin n° 406, p. 568-581, 1996.
[4] Mercier D.-J., « L'algèbre dans la correction des erreurs », A.P.M.E.P., Bulletin n° 415, p. 173-191, 1998.
[5] Querré J., « Cours d'Algèbre », Maîtrise de Mathématiques, Masson, 1976.
[6] Rolland R. et le Groupe de Travail sur la Liaison Lycées-Université de l'IREM de Marseille, « Cours et activités en arithmétique pour les classes de terminales », disponible sur le net à l'adresse http://www.irem.univ-mrs.fr, 1998. cf. Bulletin n° 417, p. 513-514.