TD Cryptographie

ENSSAT

03/02/2021

Exercice 1 – Critères de divisibilité en base 10

Soit a un entier naturel, on note $a_0, a_1, \ldots, a_n$ les chiffres de a dans le système de numération décimal, *i.e.* les $a_i \in [\![0,9]\!]$ sont tels que :

$$a = \sum_{k=0}^{n} a_k 10^k$$

Il s'agit ici de *démontrer* certaines CNS de divisibilité (les 3 premières sont très connues, mais la quatirème est un peu moins classique).

1. Divisibilité par 2 ou par 5

En utilisant $10 \equiv 0$ modulo 2 ou 5, démontrer que le reste de la division euclidienne de a par 2 ou par 5 est le même que le reste de la division de a_0 par 2 ou par 5. En déduire le critère classique de divisibilité par 2 ou 5.

2. Divisibilité par 4 ou par 25

Utiliser la méthode précédente pour obtenir un critère simple de divisibilité par 4 ou 25.

3. Divisibilité par 3 ou par 9

En utilisant $10 \equiv 1$ modulo 3 ou 9, démontrer que le reste de la division de a par 3 ou par 9 est le même que le reste de la division de $a_n + a_{n-1} + \ldots + a_0$ par 3 ou par 9, et retrouver ainsi le critère classique de divisibilité par 3 ou par 9.

4. Divisibilité par 11

En vous inspirant de la méthode précédente, obtenir un critère simple de divisibilité par 11.

Corrigé

Cette exercice est un exercice de manipulation des congruences.

1. **Divisibilité par** 2 **ou** 5. Puisque 2 et 5 divisent 10, on peut écrire $10 \equiv 0 \mod 2$ et $10 \equiv 0 \mod 5$. Ainsi, par propriété des congruences :

   $$\forall\, n \in \mathbb{N}^*,\ 10^n \equiv 0 \mod 2 \quad \text{et} \quad 10^n \equiv 0 \mod 5$$

   Notons alors $a = \sum_{k=0}^{n} a_k 10^k$. Alors, toujours par propriété des congruences :

   $$\begin{aligned} a &\equiv a_0 + 10a_1 + \ldots + 10^n a_n \mod 2 \\ &\equiv a_0 \mod 2 \text{ d'après ce qui précède} \end{aligned}$$

   Ceci est également valable modulo 5. On en déduit le résultat classique : un nombre est divisible par 2 (resp. par 5) si et seulement si son chiffre des unités est divisible par 2 (resp. par 5), c'est-à-dire si et seulement si son chiffre des unités est pairs (resp. est égal à 0 ou 5).
2. **Divisibilité par** 4 **ou** 25. On procède de la même manière, en constatant que 4 et 25 divisent 100. Ainsi, $100 \equiv 0 \mod 4$ et $100 \equiv 0 \mod 25$. Alors, pour tout $n \geqslant 2$:

   $$10^n = 10^2 \times 10^{n-2} = 100 \times 10^{n-2} \equiv 0 \mod 4(\text{ ou } 25)$$

Par le même raisonnement que précédemment :

$$\begin{aligned} a &\equiv a_0 + 10a_1 + \sum_{k=2}^{n} a_k 10^k \mod 4 \\ &\equiv a_0 + 10a_1 \mod 4 \equiv \overline{a_1 a_0} \mod 4 \end{aligned}$$

Ceci étant également valable module 25. Ainsi, a est divisible par 4 ou 25 si et seulement si le nombre composé de ses deux derniers chiffres (dizaine et unité) est également divisible par 4 ou 25. Pour 25, par exemple, cela signifie que a est divisible par 25 si et seulement si il termine par 00, 25, 50 ou 75.

3. **Divisibilité par** 3 **ou** 9. On constate que $10 = 3 \times 3 + 1 \equiv 1 \mod 3$ (de même, $10 = 9 + 1 \equiv 1 \mod 9$). Par propriété des congruences, pour tout entier $n \geqslant 1$:

$$10^n \equiv 1 \mod 3 \quad \text{et} \quad 10^n \equiv 1 \mod 0$$

On peut alors écrire :

$$\begin{aligned} a &\equiv a_0 + \sum_{k=1}^{n} a_k 10^k \mod 3 \\ &\equiv a_0 + \sum_{k=1}^{n} a_k 1 \mod 3 = \sum_{k=0}^{n} a_k \mod 3 \end{aligned}$$

Ceci étant également valable pour 9. On obtient le critère classique : a est divisible par 3 (resp. 9) si et seulement si la somme de ses chiffres est divisible par 3 (resp. 9)

4. **Critère de divisibilité par** 11. L'idée est la même, en constatant que $10 \equiv -1 \mod 11$. Ainsi, pour tout entier $n \geqslant 1$:

$$10^n \equiv (-1)^n \mod 11$$

On obtient alors

$$\begin{aligned} a &\equiv a_0 + \sum_{k=1}^{n} a_k 10^k \mod 11 \\ &\equiv a_0 + \sum_{k=1}^{n} (-1)^k a_k \mod 11 \equiv \sum_{k=0}^{n} (-1)^k a_k \mod 11 \end{aligned}$$

On obtient le critère suivant : a est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11. Par exemple, 863819 est divisible par 11. En effet : 9−1+8−3+6−8 = 11 qui est bien divisible par 11.

Exercice 2 – La plus simple des équations diophantiennes

On appelle équation diophantienne toute équation polynomiale (à plusieurs inconnues en général) dont on cherche les inconnues dans $\mathbb{Z}$. On rencontre notamment ce type d'équation lors de l'étude de la cryptanalyse d'un système. On va ici étudier l'équation diophantienne à deux inconnues :

$$a x + b y = c,\ (x, y) \in \mathbb{Z}^2$$

où a, b, c sont trois entiers relatifs fixés avec $(a, b) \neq (0, 0)$.

1. Démontrer qu'une condition nécessaire pour que (4.) ait des solutions est : PGCD(a, b) divise c.
2. Réciproquement supposons que PGCD(a, b) divise c. Justifier que l'on peut supposer que, dans l'équation (4.), les entiers a et b sont premiers entre eux.
   Comment obtenir alors une solution particulière de (4.) (on ne demande pas les calculs) ?
   En déduire la solution générale de (4.).
3. Appliquer cette méthode à la résolution de l'équation diophantienne

$$15x - 6y = 9$$

Corrigé

1. Si l'équation (1) admet au moins une solution, il existe $(x, y) \in \mathbb{Z}^2$ tels que
$$a x + b y = c$$
Notons $d = \text{PGCD}(a, b)$. d divise a et b, donc divise $a x + b y$, c'est-à-dire que d divise c.
2. Réciproquement, si c divise d, et quitte à diviser par d, on obtient l'équation
$$\frac{a}{d} x + \frac{b}{d} y = \frac{c}{d}$$
où $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $c' = \frac{c}{d}$ sont des entiers. Par définition du PGCD :
$$\text{PGCD}(a, b) = \text{PGCD}\left(d a', d b'\right) = d\,\text{PGCD}(a', b')$$
et donc $\text{PGCD}(a', b') = 1$. Ainsi, on peut supposer que a et b sont premiers entre eux, quitte à diviser l'équation par le PGCD de a et b.
On peut alors obtenir un couple (u, v) vérifiant $a u + b v = 1$ (par l'algorithme d'Eculide étendu), et alors
$$a(c u) + b(c v) = c$$
et le coupe $(c u, c v)$ est solution de (1).
Connaissant une solution particulière de (1), qu'on note (x_0, y_0), on en déduit, par soustraction, que (x, y) vérifie (1) si et seulement si
$$a(x - x_0) = b(y_0 - y)$$
Puisqu'on a supposé a et b premiers entre eux, cela indique que a divise $y_0 - y$ (théorème de Gauss) et donc que $y = y_0 - k a$ avec $k \in \mathbb{Z}$. En injectant dans l'équation précédente, on a alors
$$a(x - x_0) = b k a \iff x = x_0 + k b$$
Ainsi l'ensemble des solutions est de (1) est
$$\mathcal{S} = \left\{(x_0 - k a, y_0 + k b), \quad k \in \mathbb{Z}\right\}$$
3. Remarquons que $\text{PGCD}(15, 6) = 3$. Ainsi
$$15x - 6y = 9 \Leftrightarrow 5x - 2y = 3$$
5 et 2 sont premiers entre eux. On applique l'algorithme d'Euclide étendue pour une obtenir une solution, ou alors on constate que $(1, 1)$ est une solution particulière évidente. Alors, par soustraction
$$5x - 2y = 3 \Leftrightarrow 5(x-1) - 2(y-1) = 0 \Leftrightarrow 5(x-1) = 2(y-1)$$
5 et 2 sont premiers entre eux. D'après le théorème de Gauss, on en déduit que 5 divise $y - 1$ et donc qu'il existe $k \in \mathbb{Z}$ tel que $y - 1 = 5k$, c'est-à-dire $y = 1 + 5k$. En injectant dans l'équation précédente, on obtient
$$5(x-1) = 2 \times 5k \Leftrightarrow x = 1 + 2k$$
Ainsi, l'ensemble des solutions est
$$\mathcal{S} = \{(1 + 2k, 1 + 5k), \quad k \in \mathbb{Z}\}$$

Exercice 3 – Raisonnement de congruence

Pour $n \in \mathbb{N}$ écrit en base 10, on note $f(n)$ la somme des chiffres de n.
Soit $\text{N} = 4444^{4444}$. Calculer $\left(f \circ f \circ f\right)(\text{N})$.

Corrigé

Remarquons que, en majorant grossièrement :

$$4444^{4444} < 10000^{4444} = 10^{17776}$$

Donc 4444^{4444} possède moins de 17776 chiffres. Donc

$$\begin{aligned} f\left(4444^{4444}\right) &\leqslant f(999\cdots999) = 17776\times 9 < 160000 \\ \text{puis } f\circ f\left(4444^{4444}\right) &\leqslant f(999999) = 54 \\ \text{et } f\circ f\circ f\left(4444^{4444}\right) &< f(59) = 5+9 = 14 \end{aligned}$$

On doit donc trouver un moyen de trouver l'entier entre 1 et 13 qui est égal $f\circ f\circ f(\mathrm{N})$. Utilisons une propriété usuelle de la division par 9 : un nombre N est congrus à sa somme de chiffre modulo 9. Ainsi

$$f(\mathrm{N}) \equiv f\circ f(\mathrm{N}) \equiv f\circ f\circ f(\mathrm{N}) \equiv \mathrm{N} \mod 9$$

Or $4444 \equiv 7 \mod 9$, donc $4444^3 \equiv 1 \mod 9$. Ainsi

$$4444^{4444} = 4444^{1481\times 3}\times 4444 \equiv 1^{1481}\times 7 = 7 \mod 9$$

Ainsi $f\circ f\circ f(\mathrm{N}) \equiv 7 \mod 9$.

Le seul nombre entier congru à 7 modulo 9 dans l'intervalle $[\![1;13]\!]$ étant 7, on en déduit donc que

$$f\circ f\circ f(\mathrm{N}) = 7$$

Exercice 4 – Analyse de l'algorithme d'Euclide

On note (r_k) la suite des restes calculée lors de la détermination du PGCD de a et b, avec $a \geqslant b > 0$, $r_{-1} = a$, $r_0 = b$, et $r_{\mathrm{N}} = 0$ (premier reste nul), et $q_1, \ldots, q_{\mathrm{N}}$ les quotients successifs.

1. (a) Écrire (cf. CM) la relation de récurrence vérifiée par la suite $(r_k)_{k\in[\![0,\mathrm{N}-1]\!]}$
   (b) En déduire que $q_k \geqslant 1$ pour $k = 1, \ldots, \mathrm{N}-1$ et $q_{\mathrm{N}} \geqslant 2$.
2. Il s'agit de calculer une borne pour le nombre N de divisions euclidiennes nécessaire à la terminaison de l'algorithme d'Euclide. Soit $\varphi = \dfrac{1+\sqrt{5}}{2}$ le nombre d'or.
   (a) Démontrer par « récurrence descendante » sur k que
   $$\forall k \in [\![0, \mathrm{N}-1]\!] \quad r_k \geqslant \varphi^{\mathrm{N}-1-k}$$
   (b) En déduire que le nombre N de divisions euclidiennes de l'algorithme d'Euclide appliqué à a et b vérifie
   $$\mathrm{N} \leqslant \log_\varphi(b) + 1$$
   (c) Que dire de l'efficacité de l'algorithme d'Euclide ?
   (d) Même question pour l'algorithme d'Euclide étendu.

Corrigé

1. (a) D'après l'algorithme d'Euclide, on a, pour $1 \leqslant i \leqslant \mathrm{N}$:
   $$r_{i-2} = q_i\, r_{i-1} + r_i$$
   (b) Rappelons un élément important : la suite des (r_i) est à valeur entière strictement décroissante et atteint 0 (ce qui explique la terminaison de l'algorithme). En particulier, puisque r_{N} est le premier reste nul, on peut assurer que la suite $(r_i)_{0\leqslant i\leqslant \mathrm{N}-1}$ est strictement décroissante.

Si $q_i = 0$ (avec $1 \leqslant i \leqslant N-1$), cela signifie que $r_{i-2} = r_{i-1}$ (puisque q_i est le quotient de la division euclidienne de r_{i-2} par r_{i-1}. Ce qui est d'absurde d'après la stricte décroissance des (r_i).
Si $q_N = 1$, on a donc $r_{N-2} = r_{N-1} + r_N = r_{N-1}$ car $r_N = 0$; à nouveau cela est absurde puisque (r_i) est strictement décroissante jusqu'au rang N.

2. (a) Remarquons que φ vérifie la relation $\varphi^2 = 1+\varphi$ (c'est l'une des deux racines du polynôme $X^2 - X - 1$.
On va procéder par récurrence descendante forte. Pour $k = N-1$, alors $\varphi^{N-1-k} = 1$ et on a, par construction, $r_{N-1} \geqslant 1$ (et $r_N = 0$ premier reste nul).
Par hérédité, supposons que la relation $r_i \geqslant \varphi^{N-1-i}$ soient valables pour tout $k \leqslant i \leqslant N-1$.
Montrons que le résultat est vrai pour r_{k-1} :

$$\begin{aligned} r_{k-1} &= q_{k+1} r_k + r_{k+1} \\ &\geqslant q_{k+1}\varphi^{N-1-k} + \varphi^{N-1-(k+1)} \text{ par hypothèse de récurrence} \\ &\geqslant \varphi^{N-1-k} + \varphi^{N-k-2} \text{ car } q_k \geqslant 1 \\ &\geqslant \varphi^{N-k-2}(\varphi+1) \\ &\geqslant \varphi^{N-k-2)}\varphi^2 \text{ car } \varphi^2 = \varphi+1 \\ &\geqslant \varphi^{N-k} = \varphi^{(N-1)-(k-1)} \end{aligned}$$

Par récurrence descendante, on a donc bien le résultat.

(b) Puisque $r_0 = b$, on a alors :

$$\begin{aligned} r_0 = b \Rightarrow b &\geqslant \varphi^{N_1} \\ &\Rightarrow \ln(b) \geqslant (N-1)\ln(\varphi) \\ &\Rightarrow N \leqslant \log_\varphi(b) + 1 \text{ où } \log_\varphi(b) = \frac{\ln(b)}{\ln(\varphi)} \text{ (car } \ln(\varphi) > 0) \end{aligned}$$

(c) L'algorithme est assez efficace. Par exemple, pour $b = 100000$, on a $N \leqslant 30$.

(d) Pour Euclide étendu, c'est aussi efficace, parce que le nombre N ne dépend que des divisions euclidiennes successives : on obtient, en plus, u et v vérifiant $au + bv = 1$.

Exercice 5 – L'indicateur d'Euler

1. Calculer $\varphi(24)$.
2. Confirmer votre résultat en déterminant les éléments inversibles modulo 24 (*i.e.* les éléments inversibles de l'anneau $\frac{\mathbb{Z}}{24\mathbb{Z}}$). Quel est l'inverse de 5 ?
3. Ces éléments sont aussi les générateurs du groupe additif $\frac{\mathbb{Z}}{24\mathbb{Z}}$. À titre d'exemple, retrouver tous les éléments de $\frac{\mathbb{Z}}{24\mathbb{Z}}$) à partir de 5.

Corrigé

1. Première méthode : on écrit tout nombre de 1 à 23, et on enlève ceux qui ne sont pas premier avec 24. Cela donne :

$$1, 5, 7, 11, 13, 17, 19, 23$$

Ainsi, $\varphi(24) = 8$.
Remarquons que $24 = 3 \times 2^3$. Puisque 3 et 2 sont premiers entre eux, on a

$$\begin{aligned} \varphi(24) &= \varphi(3)\varphi(2^3) \\ &= (3-1)(2^3 - 2^2) = 8 \end{aligned}$$

2. Les inversibles de $\mathbb{Z}/24\mathbb{Z}$ sont les nombres entiers premiers avec 24. Il y a

$$\{1,5,7,11,13,17,19,23\}$$

.
5 est inversible car premier avec 24 et son inverse est lui-même : $\overline{5}\times\overline{5}=\overline{25}=\overline{1}$ dans $\mathbb{Z}/24\mathbb{Z}$.
3. 5 est un générateur de $(Z/24\mathbb{Z},+)$ car inversible dans $(\mathbb{Z}/24\mathbb{Z},\times)$. Par addition modulo 24 successives :

$$\{5,10,15,20,1,6,11,16,21,2,7,12,17,22,3,8,13,18,23,4,9,14,19,0\}$$