TD Arithmétique

LSI 1

1 Critères de divisibilité en base 10

Soit a un entier naturel, on note $a_0, a_1, \dots, a_n$ les chiffres de a dans le système de numération décimal, *i.e.*

$$a = a_n a_{n-1} \dots a_0 = \sum_{k=0}^{n} a_k 10^k$$

Il s'agit ici de *démontrer* certaines CNS de divisibilité (les 3 premières sont connues depuis l'école primaire, mais la 4-ème est moins classique).

1.1 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.

1.2 Divisibilité par 4 ou par 25

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

1.3 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 $a_n + a_{n-1} + \dots + a_0$ par 3 ou par 9, et retrouver ainsi le critère classique de divisibilité par 3 ou par 9, ainsi que "la preuve par 9".

1.4 Divisibilité par 11

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

2 La plus simple des équations diophantiennes

On appelle équation diophantienne toute équation polynômiale (à plusieurs inconnues en général) dont on cherche les inconnues dans $\mathbb{Z}$. Ce type d'équation se rencontre fréquemment dans les applications de l'arithmétique (en particulier en cryptographie). On va ici étudier l'équation diophantienne à deux inconnues :

$$ax + by = c, \ (x, y) \in \mathbb{Z}^2 \tag{1}$$

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

1. Démontrer qu'une condition nécessaire pour que (1) 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 (1), les entiers a et b sont premiers entre eux.
   Comment obtenir alors une solution particulière de (1) (on ne demande pas les calculs) ?
   En déduire la solution générale de (1).
3. Appliquer cette méthode à la résolution de l'équation diophantienne

$$15x - 6y = 9$$

2.1 Application

Résoudre dans $\mathbb{Z}^2$ les équations suivantes : $5x - 18y = 4$ et $6x + 15y = 28$.

3 Algorithme d'Euclide

3.1 Exercice 1

Déterminer à l'aide de l'algorithme d'Euclide étendu le pgcd d de $a = 1234$ et $b = 832$, et deux entiers u et v tels que $d = au + bv$.

3.2 Analyse de l'algorithme d'Euclide

On utilise les notations du cours pour l'algorithme d'Euclide. On note donc (r_k) la suite des restes calculée lors de la détermination du PGCD de a et b, avec $a \geq b > 0$, $r_{-1} = a$, $r_0 = b$, et $r_N = 0$ (premier reste nul), et $q_1, \ldots, q_N$ les quotients successifs.

1. (a) Écrire la relation de récurrence vérifiée par la suite $(r_k)_{k\in\{0,\ldots,N-1\}}$
   (b) En déduire que $q_k \geq 1$ pour $k = 1, \ldots, N-1$ et $q_N \geq 2$.
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 $\phi = \frac{1+\sqrt{5}}{2}$ le nombre d'or.
   (a) Démontrer par "récurrence descendante" sur k que
   $$\forall k \in \{0, \ldots, N-1\},\ r_k \geq \phi^{N-1-k}$$
   (b) En déduire que le nombre N de divisions euclidiennes de l'algorithme d'Euclide appliqué à a et b vérifie
   $$N \leq \log_\phi(b) + 1$$
   (c) Que dire de l'efficacité de l'algorithme d'Euclide ?
   (d) Même question pour l'algorithme d'Euclide étendu.