Licence 3 MIASHS, parcours informatique-SHS Cryptographie (UE MI0C601T)

Feuille n°1 — L'arithmétique, c'est fantastique !

emmanuel,philippe___bureaux GS256 & 203___hallouin@univ-tlse2.fr,philippe.moustrou@univ-tlse2.fr___Espace IRIS : MI0C601T___**hallouin,moustrou**

Exercice 1 : On s'étend sur Euclide

1. Pour les couples (a, b) suivants, déterminer $\operatorname{pgcd} a, b$ ainsi que les coefficients de Bézout associés au moyen de l'algorithme d'Euclide étendu :

a. $a = 103$, $b = 30$
b. $a = 693$, $b = 385$
c. $a = 81$, $b = 191$
d. $a = 676$, $b = 416$
e. $a = 56$, $b = 151$
f. Vos deux nombres à trois chiffres préférés.

2. Écrire et implémenter un algorithme qui, étant donné deux entiers a et b, retourne leur pgcd ainsi qu'une relation de Bézout, permettant de vérifier les calculs précédents.

Exercice 2 : Congruences modulo n

Pour x, y, n trois entiers, on dit que x est **congru** à y modulo n si n divise la différence $x - y$; dans ce cas, on note :

$$x \equiv y \pmod{n}$$

1. Montrer que pour tout $m \in \mathbb{Z}$ et tout $n \in \mathbb{N}$, il existe $r \in \mathbb{N}$ tel que :

$$m \equiv r \pmod{n} \qquad \text{et} \qquad 0 \leqslant r < n$$

2. Montrer que cette relation est réflexive, symétrique et transitive, c'est-à-dire :

$$\begin{aligned} &x \equiv x \pmod{n} \\ &x \equiv y \pmod{n} \quad \Longrightarrow \quad y \equiv x \pmod{n} \\ &x \equiv y \pmod{n} \text{ et } y \equiv z \pmod{n} \quad \Longrightarrow \quad x \equiv z \pmod{n} \end{aligned}$$

où x, y, z sont des entiers et n un modulus non nul.

3. Vérifier que cette relation est compatible avec l'addition et la multiplication ; autrement dit, étant donnés $x, y, x', y', n \in \mathbb{Z}$, montrer que l'on a les implications suivantes :

- si $x \equiv y \pmod{n}$ et si $x' \equiv y' \pmod{n}$ alors $x + x' \equiv y + y' \pmod{n}$;
- si $x \equiv y \pmod{n}$ et si $x' \equiv y' \pmod{n}$ alors $xx' \equiv yy' \pmod{n}$.

4. À votre avis, si $xy \equiv xz \pmod{n}$, a-t-on $y \equiv z \pmod{n}$?

Exercice 3 : Quelle taille ?

Convenons que la **taille** d'un entier n est la longueur du tableau dans lequel est stocké sa décomposition en base 2.

1. Quelle est la taille des nombres suivants ?

a. n, pour $1 \leqslant n \leqslant 15$,
b. 45,
c. 167,
d. 32769,
e. 65535.

2. Exprimer cette taille en fonction de $\log_2 n$.

3. Soit a, b et n des entiers avec $n \geqslant 1$.

a. Que peut-on dire de la taille de $a + b$ en fonction de celles de a et b ?
b. Que peut-on dire de la taille de $a \times b$ en fonction de celles de a et b ?
c. Que peut-on dire des tailles du reste et du quotient de la division de a par b (quand $b \neq 0$) en fonction de celles de a et b ?
d. Que peut-on dire de la taille de a^n en fonction de celle de a ?

Exercice 4 : Retour à l'école primaire

L'idée de cet exercice est de revenir sur les opérations élémentaires des entiers du point de vue de la complexité.

1. En vous basant sur les techniques que vous avez vues à l'école primaire, donner la complexité des opérations élémentaires entre deux entiers $\leqslant n$ suivante :

Opération	Complexité en fonction de a et b	Complexité en fonction de n
$a + b$		
$a - b$		
$a \times b$		
$a \div b$		
$\text{pgcd}(a, b)$		

Note : pour le calcul du pgcd, on utilise l'algorithme d'Euclide.

2. Quelle est la complexité de l'algorithme naïf de factorisation de n ?

Exercice 5 : Actualités : pouvoir d'achat... mais non de calcul

Soit p et q deux premiers chacun de taille 256 bits. On pose $n = p \times q$.

1. Quelle est la taille de n ?

2. Quel est le coût de la somme de deux entiers $\leqslant n$? Et celui du reste de la division euclidienne de cette somme par n ?

3. Pour $m \leqslant n$, quel est le coût du calcul du $\text{pgcd}(m, n)$ accompagné des coefficients de Bezout ?

4. Quel est le coût de l'algorithme naïf permettant de factoriser n ?

Exercice 6 : Le coût (de la vie)

Soit $n \in \mathbb{Z}$ un entier dont l'écriture binaire compte 512 chiffres.

1. Quelle est la taille de l'entier n ?

2. Combien de divisions doit-on effectuer au maximum pour factoriser cet entier n (si c'est possible) avec l'algorithme naïf de factorisation ?

3. Combien d'opérations au maximum sont-elles nécéssaires pour ajouter deux éléments $\leqslant n$? Puis calculer le reste de cette somme modulo n ?