Licence 3 – MHT633 Université Bordeaux 1
2009/2010

Feuille 2 : Complexité et arithmétique

Exercice 1. Soit N un entier naturel non nul.

1. Soit $n = \log_2 N$ et $n' = \log_e N$. Montrer qu'un algorithme en $\mathcal{O}(n)$ est aussi en $\mathcal{O}(n')$ et réciproquement.
2. Quelle est la complexité de l'addition modulo N, c'est à dire l'algorithme qui prend en entrée (A, B) avec $0 \leq A < N$, $0 \leq B < N$ et retourne C tel que $0 \leq C < N$ et $C \equiv A + B \pmod{N}$? Quelle est la complexité de la multiplication modulo N ?
3. Le chiffrement affine envoie $x \in \mathbb{Z}/N\mathbb{Z}$ sur $ax + b$ où $a, b \in \mathbb{Z}/N\mathbb{Z}$. Quelle est la complexité de cet algorithme de chiffrement ?
4. Le chiffrement de Hill envoie $x \in (\mathbb{Z}/N\mathbb{Z})^\ell$ sur xM où $M \in GL_\ell(\mathbb{Z}/N\mathbb{Z})$ avec ℓ un entier naturel non nul. Quelle est celle de cet algorithme de chiffrement ?
5. Le chiffrement par décalage envoie $x \in \mathbb{Z}/N\mathbb{Z}$ sur $x + k$ où $k \in \mathbb{Z}/N\mathbb{Z}$. On dispose d'un couple (m, c) message clair, message chiffré correspondant, pour ce chiffrement. On souhaite retrouver la clef de chiffrement. Quelle est la complexité dans le pire cas de l'attaque naïve par recherche exhaustive ? Quelle est celle de l'attaque « intelligente » ?

Exercice 2. On se place dans $\mathbb{Z}/23\mathbb{Z}$.

1. Calculer 2^7 et 3^8 par l'algorithme d'exponentiation modulaire.
2. Combien avez-vous effectué de multiplications modulaires dans chacun des cas ? Dans le cas général, combien faut il de multiplications modulaires pour calculer a^k dans $\mathbb{Z}/N\mathbb{Z}$ avec k en entier non nul de ℓ bits et N un entier naturel non nul.

Exercice 3. Montrez qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

Exercice 4. Montrez qu'un entier est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres dans son écriture décimale est divisible par 4.

Exercice 5. Trouvez le pgcd et une relation de Bezout pour les couples (a, b) suivants :

$$(34, 21), \quad (136, 51), \quad (481, 325), \quad (8771, 3206)$$

puis répondez aux questions

1. a est-il inversible modulo b ? Si oui quel est son inverse ?
2. b est-il inversible modulo a ? Si oui quel est son inverse ?

Exercice 6.

1. Quels sont les inversibles de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$?
2. Si p est premier, quels sont les inversibles de $\mathbb{Z}/p^2\mathbb{Z}$?

Exercice 7. Résoudre les équations suivantes :

1. $2x = 37$ dans $\mathbb{Z}/21\mathbb{Z}$,
2. $5x = 15$ dans $\mathbb{Z}/25\mathbb{Z}$,
3. $3x = 7$ dans $\mathbb{Z}/18\mathbb{Z}$.

Explicitez la résolution générale de l'équation $ax = b$ dans $\mathbb{Z}/c\mathbb{Z}$.

Exercice 8. Résoudre les systèmes d'équations :

$$(a)\ \begin{cases} x + y = 6 \\ 2x - y = 8 \end{cases}, \quad x, y \in \mathbb{Z}/11\mathbb{Z} \qquad (b)\ \begin{cases} 3x + 17y = 9 \\ 9x + 6y = 6 \end{cases}, \quad x, y \in \mathbb{Z}/51\mathbb{Z}.$$

Explicitez les opérations transformant un système linéaire en un système équivalent lorsque les coefficients sont dans un anneau A (commutatif unitaire).

Exercice 9. Résoudre dans $\mathbb{Z}$

$$\begin{cases} 2x \equiv 37 \pmod 5, \\ 3x \equiv 48 \pmod 7. \end{cases}$$

Exercice 10. Théorème chinois

1. Soit $a, b \in \mathbb{Z}$ premiers entre eux. On considère l'application suivante :

$$\begin{array}{cccc} \Phi & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & x \mod ab & \longmapsto & (x \mod a, x \mod b) \end{array}$$

Montrer que Φ est un isomorphisme d'anneaux.

2. Expliciter Φ^{-1}.

Exercice 11.

Soit $c \in \mathbb{Z}$, montrer que $\frac{1}{24}(c^6 + 3c^4 + 12c^3 + 8c^2)$ est un entier. (Indication : Montrer que si c est un inversible de $\mathbb{Z}/8\mathbb{Z}$ alors $c^2 = 1$.)

Exercice 12. Indicatrice d'Euler

Soit φ la fonction indicatrice d'Euler définie sur $\mathbb{N}$ par

$$\varphi(n) = |\{k \in \mathbb{N} \text{ tel que } 1 \leq k \leq n \text{ et } \operatorname{pgcd}(k, n) = 1\}|$$

1. Montrer que $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.
2. Soit p un nombre premier et $k \in \mathbb{N}$. Calculer $\varphi(p)$ et $\varphi(p^k)$.
3. Se servir du théorème chinois pour établir que si

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

est la décomposition en produit de facteurs premiers de n on a

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Exercice 13. Le groupe $(\mathbb{Z}/pq\mathbb{Z})^\times$

Soit p et q deux nombres premiers distincts et $n = pq$.

1. Déterminer les inversibles de $\mathbb{Z}/n\mathbb{Z}$.
2. Calculer l'ordre du groupe $(\mathbb{Z}/pq\mathbb{Z})^\times$.
3. Faire le lien avec l'indicatrice d'Euler.

Exercice 14. Ordre d'un élément

1. Si $x^a = 1$ pour un entier naturel a et un élément x de $(\mathbb{Z}/n\mathbb{Z})^\times$, montrer que l'ordre de x divise a.
2. Montrer que pour tout x de $\mathbb{Z}/p\mathbb{Z}$ on a $x^p = x$.
3. Montrer que pour tout x de $(\mathbb{Z}/n\mathbb{Z})^\times$ on a $x^{\phi(n)} = 1$.
4. En déduire une façon de calculer l'inverse de x dans $(\mathbb{Z}/n\mathbb{Z})^\times$, qui ne fasse pas appel à l'algorithme d'Euclide étendu. Application : calcul de l'inverse de 7 dans $(\mathbb{Z}/15\mathbb{Z})^*$.

Exercice 15. Un multiple de 633 (DS 2010)

Le but de l'exercice est de trouver un multiple de 633 dont l'écriture en base 10 ne comporte que des 3.

1. Soit $b \in \mathbb{N}\backslash\{0,1\}$, donner la définition de l'écriture en base b d'un entier naturel.
2. Soit n un entier naturel non nul dont l'écriture en base 10 ne comporte que des 3. Montrer que n s'écrit :
$$3\left(\frac{10^{k+1}-1}{9}\right)$$
pour un entier naturel k.
3. En déduire que n est un multiple de 633 si et seulement si $10^{k+1} \equiv 1 \pmod{211}$.
4. Montrer que 211 est premier. En déduire un entier n convenable.
5. Adapter cette méthode pour trouver un multiple de 561 dont l'écriture décimale ne comporte que des 3.