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. Quelle est la complexité de l'algorithme de chiffrement affine dans $\mathbb{Z}/N\mathbb{Z}$? Quelle est celle de l'algorithme de chiffrement de Hill dans $(\mathbb{Z}/N\mathbb{Z})^\ell$ avec ℓ un entier naturel non nul ?
4. On dispose d'un couple (m, c) message clair, message chiffré correspondant, pour un chiffrement par décalage dans $\mathbb{Z}/N\mathbb{Z}$. 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. Soit a un nombre rationnel tel que $18a$ et $25a$ sont des nombres entiers. Montrez que a est aussi entier.

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

Exercice 5. Trouvez tous les entiers p et q tels que $4p + 7q = pq$.

Exercice 6. Soit a et b des entiers distincts.

1. Montrez que $a-b$ divise a^2-b^2 et déterminez le quotient.
2. Montrez que $a-b$ divise a^3-b^3 et déterminez le quotient.
3. Montrez que $a-b$ divise a^n-b^n pour tout n
4. Montrez que $a+b$ divise $a^{2n+1}+b^{2n+1}$ pour tout n.
5. Trouvez la factorisation en nombres premiers de $5^{10}-2^{10}$.

Exercice 7. Nombres de Fermat

1. Vérifiez que les nombres $3=2+1$, $5=2^2+1$, $17=2^4+1$, $257=2^8+1$ sont premiers. On pourrait aussi vérifier que $65537=2^{16}+1$ est premier.
2. Montrez que, si $N=2^k+1$ est premier, alors k est nécessairement une puissance de 2.
3. Fermat conjecturait que les nombres de la forme $2^{2^n}+1$ sont premiers. Cela est vrai pour $n=0,1,2,3,4$ mais n'est pas vrai pour $n=5$. Montrez, à l'aide des observations suivantes, que 641 divise $2^{2^5}+1$:
   (a) $641=2^9+2^7+1$ donc $2^7\cdot 5\equiv -1 \pmod{641}$,
   (b) $2^4\equiv -5^4 \pmod{641}$.

Exercice 8. 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 9. 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 10. La date de naissance d'Alice est telle que le jour multiplié par 12 ajouté au mois multiplié par 31 fait 442. Déterminez la.

Exercice 11.

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 12. 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 13. 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 14. Résoudre dans $\mathbb{Z}$

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

Exercice 15. Résoudre les équations du second degré :

1. $x^2 + x + 7 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$.
2. $x^2 - 2x + 3 = 0$ dans $\mathbb{Z}/4\mathbb{Z}$.
3. $x^2 - 4x + 3 = 0$ dans $\mathbb{Z}/12\mathbb{Z}$.

Explicitez une méthode de résolution générale.