Licence 3 – 4TTI603U Université de Bordeaux
2024/2025

Feuille 2 : Complexité, arithmétique et algorithme d'Euclide

Exercice 1. Soient des entiers $m \geq n \geq 1$ et $a \geq 2$.

1. Soit r le reste de la division euclidienne de m par n. Montrer que le reste de la division de $a^m - 1$ par $a^n - 1$ est $a^r - 1$.
   Le cas où $m = n$ est trivial.
   Supposons que $m > n$, alors $m = qn + r$ avec $0 \leqslant r < n$.

$$\begin{aligned} a^m - 1 = a^{qn+r} - 1 &= a^{qn+r} - a^r + a^r - 1 \\ &= a^r(a^{qn} - 1) + (a^r + 1) \\ &= a^r(a^n - 1)(a^{q-1} + \cdots a + 1) + (a^r - 1) \end{aligned}$$

   En tenant compte que $0 \leqslant r < n$ alors $0 \leqslant a^r - 1 < a^n - 1$.
   Donc le reste de la division de $a^m - 1$ par $a^n - 1$ est bien $a^r - 1$.
2. En déduire que $\text{pgcd}(a^m - 1, a^n - 1) = a^{\text{pgcd}(m,n)} - 1$. On répète ce processus comme dans la division euclidienne de m par n qui nous donnera le $\text{pgcd}(m, n)$ et donc $\text{pgcd}(a^m - 1, a^n - 1) = a^{\text{pgcd}(m,n)} - 1$.
3. Retrouver ce résultat en montrant que si un entier d divise $a^m - 1$ et $a^n - 1$, alors d divise $a^{\text{pgcd}(m,n)} - 1$. Soit d un entier qui divise $a^m - 1$ et $a^n - 1$ alors d est forcément premier avec a et donc a est inversible modulo d. Il existe des entiers u, v tels que $um + vn = \text{pgcd}(m, n)$. Alors

$$a^{\text{pgcd(m,n)}} \equiv a^{um+vn} \equiv (a^m)^u \cdot (a^n)^v \equiv 1 \bmod d.$$

   Cela montre que n'importe quel diviseur de $a^m - 1$ et $a^n - 1$ est un diviseur de $a^{\text{pgcd}(m,n)} - 1$. Maintenant il suffit de montrer que n'importe quel diviseur de $a^{\text{pgcd}(m,n)} - 1$ divise aussi $a^m - 1$ et $a^n - 1$.

   On sait que $\frac{x^k-1}{x-1} = x^{k-1} + \cdots + x + 1$, alors si $e|f$ alors $a^e - 1 | a^f - 1$, donc $a^{\text{pgcd}(m,n)} - 1$ divise $a^m - 1$ et $a^n - 1$. Ce qui nous donne une preuve alternative.

Exercice 2.

1. Trouver le pgcd et une relation de Bézout pour les couples (a, b) suivants : $(136, 51)$ et $(57, 13)$.
   Commençons avec $(136, 51)$. En utilisant l'algorithme d'Euclide étendu, on trouve $\text{pgcd}(136, 51) = 17 = 1 \cdot 136 + 3 \cdot 51$.
   Calcul du PGCD et coefficients de Bézout
   On applique l'algorithme d'Euclide :

$$57 = 13 \times 4 + 5$$
$$13 = 5 \times 2 + 3$$
$$5 = 3 \times 1 + 2$$
$$3 = 2 \times 1 + 1$$
$$2 = 1 \times 2 + 0$$

   Ainsi, $\gcd(57, 13) = 1$.
   On remonte pour obtenir la combinaison linéaire :

$$1 = 3 - 1(5 - 1 \times 3) = 2 \times 3 - 1 \times 5$$
$$= 2(13 - 2 \times 5) - 1 \times 5 = 2 \times 13 - 5 \times 5$$
$$= 2 \times 13 - 5(57 - 4 \times 13)$$
$$= 22 \times 13 - 5 \times 57$$

   D'où la relation de Bézout :

$$57 \times (-5) + 13 \times 22 = 1$$

   Les coefficients de Bézout sont : x = -5, y = 22. Puis $\text{pgcd}(57, 13) = 1 = 5 \cdot 57 + 22 \cdot 13$.
2. Calculer l'inverse de 25 dans l'anneau $\mathbb{Z}/37\mathbb{Z}$. En sachant que $1 = 3 \cdot 25 - 2 \cdot 37$, alors l'inverse de 25 est 3 dans $\mathbb{Z}/37\mathbb{Z}$.
3. Donner la liste des éléments x inversibles de l'anneau $\mathbb{Z}/12\mathbb{Z}$ et de leurs inverses x^{-1}. Même question dans $\mathbb{Z}/9\mathbb{Z}$. Il faut trouver les $x \in \mathbb{Z}/12\mathbb{Z}$ tel que $\text{pgcd}(x, 12) = 1$, donc $x \in \{1, 5, 7, 11\}$

Exercice 3.

1. Trouver tous les entiers n vérifiant $2n \equiv 5 \pmod{21}$. Résolvons la congruence :

$$2n \equiv 5 \pmod{21}$$

Cherchons l'inverse de 2 modulo 21. Nous devons trouver x tel que :

$$2x \equiv 1 \pmod{21}$$

En testant, on trouve $x \equiv 11 \pmod{21}$, car $2 \times 11 = 22 \equiv 1 \pmod{21}$.
En multipliant la congruence par 11 :

$$11 \cdot 2n \equiv 11 \cdot 5 \pmod{21}$$

$$n \equiv 55 \pmod{21}$$

$$55 = 2 \times 21 + 13 \Rightarrow n \equiv 13 \pmod{21}$$

Ainsi, la solution générale est :

$$n = 13 + 21k, \quad k \in \mathbb{Z}$$

2. Déterminer tous les $x \in \mathbb{Z}/25\mathbb{Z}$ vérifiant $20x = 1$. Même question pour l'équation $20x = 10$. 20 n'est pas premier à 25, donc $20x = 1$ n'admet pas de solution.
Résolvons la congruence :

$$20x \equiv 10 \pmod{25}$$

Le PGCD $\gcd(20, 25) = 5$ divise 10, donc la congruence est soluble. Divisons par 5 :

$$4x \equiv 2 \pmod{5}$$

Cherchons l'inverse de 4 modulo 5. On trouve $4^{-1} \equiv 4 \pmod{5}$, car $4 \times 4 = 16 \equiv 1 \pmod{5}$. En multipliant par 4^{-1} :

$$x \equiv 3 \pmod{5}$$

Relevons cette solution dans $\mathbb{Z}/25\mathbb{Z}$:

$$x = 3 + 5k, \quad k \in \mathbb{Z}$$

Les solutions modulo 25 sont donc :

$$x \equiv 3, 8, 13, 18, 23 \pmod{25}$$

3. Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ vérifiant :

$$x + y \equiv 6 \pmod{11} \quad \text{et} \quad 2x - y \equiv 8 \pmod{11}.$$

Exercice 4. Trouver tous les entiers n vérifiant : $2n \equiv 3 \pmod 5$ et $3n \equiv 1 \pmod 7$.

Exercice 5. Trouver tous les entiers n vérifiant

$$\begin{cases} 5n \equiv 6 \pmod{12} \\ 2n \equiv 3 \pmod{15} \\ 2n \equiv 4 \pmod 7 \end{cases}$$

Exercice 6. Algorithme de Karatsuba.

1. Soient a et b deux entiers naturels $< 2^{2n}$ avec n un entier ≥ 1. Comment calculer ab en n'effectuant que trois multiplications d'entiers naturels $\approx 2^n$? Indication : écrire $a = 2^n a_1 + a_2$ et $b = 2^n b_1 + b_2$ puis considérer $(a_1 + a_2)(b_1 + b_2)$.
2. Soient a et b deux entiers naturels $< 2^n$ avec $n = 2^m$ pour un entier m. Proposer un algorithme calculant ab de complexité $\mathcal{O}(n^\alpha)$ avec $\alpha = \log_2(3) \approx 1.58$.

Exercice 7. 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 $m \in \mathbb{Z}/N\mathbb{Z}$ sur $am + b$ où $a, b \in \mathbb{Z}/N\mathbb{Z}$. Quelle est la complexité de cet algorithme de chiffrement ?
4. Le chiffrement de Hill envoie $m \in (\mathbb{Z}/N\mathbb{Z})^\ell$ sur mK où $K \in GL_\ell(\mathbb{Z}/N\mathbb{Z})$ avec ℓ un entier naturel non nul. Quelle est celle de cet algorithme de chiffrement ?
5. Le chiffrement par décalage envoie $m \in \mathbb{Z}/N\mathbb{Z}$ sur $m + k$ 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 8. 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 un entier non nul de ℓ bits et N un entier naturel non nul.

Exercice 9. Complexité de l'algorithme d'Euclide

Si x est un entier, on note $L(x) = E(\log_2(x)) + 1$ le nombre de bits de x. Soient a et b deux entiers tels que $a > b > 0$. On note $r_0 = a$ et $r_1 = b$. On applique l'algorithme d'Euclide à a et b de la manière suivante :

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n \end{aligned}$$

où $r_n = \text{pgcd}(a, b)$.

1. La suite des nombres de Fibonacci est définie par $F_0 = 0, F_1 = 1$, $F_i = F_{i-1} + F_{i-2}$ pour $i \geq 2$. Calculer $\text{pgcd}(F_{n+2}, F_{n+1})$ pour $n \geq 0$. Combien fait-on d'étapes et que valent les quotients ?
2. Montrer que si le calcul de $\text{pgcd}(a, b)$ utilise n divisions euclidiennes alors $b \geq F_{n+1}$. *Indication* : remonter l'algorithme.
3. Vérifier que pour tout $n \geq 2$, $F_n \geq \Phi^{n-2}$ où $\Phi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or. En déduire que l'algorithme d'Euclide appliqué à a et b s'arrête après $\mathcal{O}(L(b))$ divisions euclidiennes (Théorème de Lamé).
4. Montrer que dans l'algorithme d'Euclide le produit des quotients est majoré par a, c'est-à-dire que $q_1 q_2 \dots q_n \leq a$.
5. La division euclidienne de x par y peut se faire en $\mathcal{O}(L(y)L(q))$ opérations binaires où q est le quotient. Montrer que la complexité de l'algorithme d'Euclide est en $\mathcal{O}(L(a)L(b))$

Exercice 10. Inverser par exponentiation

1. Utiliser le fait que pour tout x de $(\mathbb{Z}/n\mathbb{Z})^\times$ on a $x^{\varphi(n)} = 1$ pour proposer 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. Quelle est la complexité de cet algorithme ?
2. Application : calcul de l'inverse de 7 dans $(\mathbb{Z}/15\mathbb{Z})^\times$.