UFR Sciences — 2023–2024
M2 Calcul Formel — Martin WEIMANN

Contrôle Terminal - Calcul Formel

Exercice 1 (Inversion et division euclidienne rapide des polynômes) Soit $\mathbb{A}$ un anneau commutatif. Etant donné $G \in \mathbb{A}[X]$, on considérera $G \mod X^N$ comme un polynôme de $\mathbb{A}[X]$ de degré $< N$. On note $M(N)$ le coût de la multiplication de deux polynômes de degrés au plus N dans $\mathbb{A}[X]$.

1. **Inversion rapide modulo X^N.** Soit N un entier et soit $G \in \mathbb{A}[x]$ tel que $G(0) = 1$.

   (a) Montrer qu'il existe un unique $H \in \mathbb{A}[x]$ de degré $< N$ tel que
   $$GH \equiv 1 \mod X^N.$$
   Penser à utiliser $(1-u)(1+u+\cdots+u^{N-1}) = 1-u^N$. On appelle H l'inverse de G modulo X^N, noté $H = G^{-1} \mod X^N$.

   (b) Soit $H = G^{-1} \mod X^N$. Montrer que le polynôme
   $$N(H) := H + (1 - GH)H \mod X^{2N}$$
   vérifie $N(H) = G^{-1} \mod X^{2N}$.

   (c) En déduire un algorithme diviser pour régner qui calcule l'inverse de G modulo X^N.

   (d) Justifier que l'on peut calculer $N(H)$ avec $2M(N) + O(N)$ opérations dans $\mathbb{A}$.

   (e) On suppose $\deg G < N$ avec N une puissance de 2. Déduire des questions précédentes que l'on peut calculer l'inverse de G modulo X^N avec $2M(N) + O(N)$ opérations dans $\mathbb{A}$.

2. **Division euclidienne rapide.** Soient $F, G \in \mathbb{A}[X]$ avec G unitaire. On note $m = \deg(F)$ et $n = \deg(G)$ et on supposera $m \geq n$.

   (a) Justifier que la division euclidienne de F par G est bien définie dans $\mathbb{A}[X]$ et rappeler le coût de l'algorithme naïf en fonction de m.

   (b) Pour $P \in \mathbb{A}[X]$ de degré d, on note $\tilde{P} = X^d P(1/X) \in \mathbb{A}[X]$ le polynôme réciproque de P. Soit Q le quotient de la division de F par G. Montrer que
   $$\tilde{F} \equiv \tilde{Q}\tilde{G} \mod X^{m-n+1}.$$

   (c) En déduire que la division euclidienne $F = QG + R$ de F par G peut se calculer selon les formules
   $$P := \tilde{F}\tilde{G}^{-1} \mod X^{m-n+1}, \qquad Q := X^{m-n}P(1/X), \qquad R := F - QG \mod X^n.$$

   (d) Conclure que la division euclidienne de F par G peut s'effectuer en $O(M(m))$ opérations dans $\mathbb{A}$.

3. **Codage et tests.** *(Sage)* On travaillera avec l'anneau $\mathbb{A} = \mathbb{Z}/8\mathbb{Z}$.

   (a) Coder l'inversion rapide modulo X^N dans $\mathbb{A}[X]$.

   (b) Tracer la courbe de complexité en testant sur un polynôme aléatoire G de degré $N-1$ vérifiant $G(0) = 1$ pour $N \in \{1, \ldots, 1000\}$.

   (c) Pour $N = 1000$, comparer les temps de l'inversion rapide et de l'inversion naïve héritée de la formule $1/(1-u) = 1 + u + u^2 + \cdots$.

   (d) Coder la division rapide dans $\mathbb{A}[X]$. Tester sur $F, G \in \mathbb{A}[X]$ aléatoires de degrés respectifs $m = 10^5$ et $n = 10^4$, avec G unitaire. Donner le temps d'exécution.

Exercice 2 (L'algorithme de Kraitchik pour la factorisation des entiers) On veut factoriser un entier N en construisant des couples d'entiers $1 \leq x, y \leq N$ tels que $x^2 \equiv y^2 \mod N$. Ceci équivaut à

$$N = \mathrm{pgcd}(x-y, N)\,\mathrm{pgcd}(x+y, N) \qquad (*)$$

qui, si N est composé et x et y sont premiers à p, conduit avec plus d'une chance sur deux à une factorisation non triviale de N. L'enjeu est de construire (vite) de tels couples (x, y).

Fixons $P = \{p_1, \ldots, p_n\}$ un ensemble de nombres premiers. On dit que $a \in \mathbb{N}$ est *P-friable* si tous ses facteurs premiers sont dans P, c'est à dire si

$$a = \prod_{j=1}^{n} p_j^{c_j}, \quad c_j \in \mathbb{N}.$$

On notera alors $v(a) := (c_1, \ldots, c_n) \in \mathbb{N}^n$.

1. On suppose que N a au moins deux facteurs premiers impairs. Justifier que l'équation $z^2 = 1 \mod N$ a au moins deux solutions non triviales (distinctes de ± 1). En déduire que si $1 \leq x, y \leq N$ sont premiers à N et vérifient $x^2 \equiv y^2 \mod N$, alors $(*)$ donne une factorisation non triviale avec plus d'une chance sur deux.

2. Soient $a_1, \ldots, a_m$ des entiers distincts P-friables, avec $m \geq n+1$. Justifier qu'il existe une combinaison $\mathbb{F}_2$-linéaire non triviale des vecteurs $v(a_i) \mod 2$.

3. En déduire qu'il existe $I \subset \{1, \ldots, m\}$ non vide tel que $\prod_{i \in I} a_i$ est un carré dans $\mathbb{Z}$.

4. Comment calculer alors $1 \leq y < N$ tel que $\prod_{i \in I} a_i \equiv y^2 \mod N$?

5. Supposons de plus les a_i de la forme $a_i = b_i^2 - N$ et notons $x = \prod_{i \in I} b_i \mod N$. Montrer que le couple x, y ainsi construit vérifie $x^2 \equiv y^2 \mod N$ et donc la relation $(*)$.

6. *(Sage)* Un exemple concret :

   (a) Ecrire une procédure qui, étant donnés P et a, retourne la liste $v(a)$ si a est P-friable, et la liste vide sinon. Bien sûr, il faut faire en sorte de ne pas utiliser la factorisation.

   (b) Soit $N = 4333801$ et soit P la liste des 9 plus petits nombres premiers. Montrer qu'il existe exactement 10 entiers

   $$[b_1, \ldots, b_{10}] = [2086\,,\ 2099\,,\ 2131\,,\ 2147\,,\ 2221\,,\ 2247\,,\ 2351\,,\ 2477\,,\ 2776\,,\ 2891].$$

   tels que $\lceil \sqrt{N} \rceil \leq b_i \leq \lceil \sqrt{N} \rceil + 10^3$ et tels que $a_i = b_i^2 - N$ est P-friable. Stocker dans une liste les quantités $(b_i, v(a_i))$.

   (c) Déterminer une base du noyau gauche de la matrice M sur $\mathbb{F}_2$ dont les lignes sont constituées des vecteurs $v(a_i) \mod 2$.

   (d) Pour chaque vecteur de la base, construire la liste $I \subset \{1, \ldots, 9\}$ correspondante tel que le vecteur $\sum_{i \in I} v(a_i)$ a ses coordonnées paires.

   (e) Pour chaque tel I, notons $(c_1, \ldots, c_9)$ les coordonnées du vecteur $\frac{1}{2} \sum_{i \in I} v(a_i) \in \mathbb{Z}^9$. Calculer

   $$x = \prod_{i \in I} b_i \mod N \qquad \text{et} \qquad y = \prod_{j=1}^{9} p_j^{c_j} \mod N$$

   puis vérifier que $x^2 \equiv y^2 \mod N$ et tester si (x, y) fournit une factorisation non triviale de N.

La difficulté est alors de choisir un ensemble P suffisamment petit pour un test de friabilité rapide, mais suffisamment gros pour une proportion suffisante de nombres friables. Mais c'est une autre histoire...

Exercice 3 (Corps finis) Deux questions indépendantes.

1. Irréductibilité dans $\mathbb{F}_2[X]$.
   (a) Quelles sont les sous-corps de $\mathbb{F}_{16}$?
   (b) Montrer que $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
   (c) Soit $Q \in \mathbb{F}_2[X]$ irréductible de degré 4. Montrer que Q a exactement deux facteurs irréductibles de degrés 2 dans $\mathbb{F}_4[X]$.
   (d) *(Sage)* Ecrire une procédure qui liste tous les polynômes irréductibles unitaires de degré donné n de $\mathbb{F}_2[X]$ (utiliser la structure d'espace vectoriel pour lister les polynômes de degrés n).
   (e) *(Sage)* Vérifier l'assertion du c) sur tous les polynômes irréductibles de degrés 4 de $\mathbb{F}_2[X]$.
2. On rappelle qu'un code cyclique sur $\mathbb{F}_p$ de longueur n est un idéal de $\mathbb{F}_p[X]/(X^n - 1)$, donc défini par un diviseur g de $X^n - 1$. Le code est dit irréductible si g l'est.
   (a) Quelle est la dimension du code engendré par g ? Déterminer une base de ce code. Déterminer une application linéaire dont la matrice est une matrice de contrôle de ce code.
   (b) Soit C un code linéaire. Montrer que la distance minimale du code C est le plus petit entier d tel que la matrice de contrôle ait d colonnes liées.
   (c) *(Sage)* Montrer qu'il n'existe aucun code cyclique irréductible sur $\mathbb{F}_3$ de longueur 10 et de distance minimale $d \geq 3$. Cela reste-t-il vrai si l'on ne suppose plus le code irréductible ?

Exercice 4 (Polynômes multivariés) Soit $\mathbb{K}$ un corps et soit $f \in \mathbb{K}[X_1, \ldots, X_n]$ un polynôme multivarié. On dit qu'un point p de la variété $f = 0$ est singulier si f et toutes ses dérivées partielles s'annulent en p. Moralement, cela signifie que la variété $f = 0$ n'est pas "lisse" au voisinage de p.

1. Soit $f = gh$ un produit de deux polynômes $g, h \in \mathbb{K}[X_1, \ldots, X_n]$. Montrer que tout point p de la variété $\{g = h = 0\}$ est un point singulier de la variété $f = 0$.
2. *(Sage)* Soit C la courbe plane paramétrée par
$$x(t) = \frac{8t^3}{(1+t^2)^3}, \qquad y(t) = \frac{(1-t^2)^3}{(1+t^2)^3}$$
   (a) Déterminer une équation implicite de C.
   (b) En déduire l'ensemble des singularités de C sur $\bar{\mathbb{Q}}$.
   (c) Tracer la courbe C *via* son équation implicite. Votre résultat est-il en accord avec le a) ?
3. *(Sage)* Considérons la surface de Cayley S d'équation
$$x^2 + y^2 + z^2 + x^2 z - y^2 z - 1 = 0.$$
   (a) Déterminer les points singuliers de S sur $\bar{\mathbb{Q}}$.
   (b) Tracer cette surface. Le dessin est-il en accord avec vos résultats ?
4. *(Sage)* Reprendre la question 2 avec la courbe paramétrée
$$x(t) = \frac{t^3 - 1}{1 + t^4}, \qquad y(t) = \frac{t^2 - 1}{1 + t^4}$$
   montrer que le graphe ne correspond pas à la réalité. Avez-vous une explication à proposer (personnellement je n'en ai pas).