Applications de l'algorithme d'Euclide sur les entiers et les polynômes

Nous allons considérer les utilisations suivantes de l'algorithme d'Euclide. Sur les entiers naturels : calculs arithmétiques. Sur les polynômes à une indéterminée sur un corps : calculs d'extensions algébriques, approximations de Padé. Nous verrons l'utilisation pour les calculs de résultants dans une séance ultérieure.

Exercice 1 - *L'algorithme d'Euclide (étendu).*

1. Rappeler la définition d'un anneau euclidien. Vérifier que $\mathbb{Z}$ et $k[X]$, où k est un corps commutatif, sont des anneaux euclidiens.
2. Décrire l'algorithme d'Euclide permettant de calculer un p.g.c.d. de deux éléments d'un anneau euclidien.
3. Comment utiliser cet algorithme pour trouver un couple de Bézout ?

Il est facile de voir que tout anneau euclidien est principal. La réciproque est fausse, comme par exemple l'anneau $\mathbb{Z}[(1+\mathrm{i}\sqrt{19})/2]$.

Exercice 2 - *Problèmes arithmétiques.*

1. Décrivez les solutions (x, y) d'une équation diophantienne de la forme $ax + by = c$.
2. Décrivez une solution (x, y, z) d'une équation diophantienne de la forme $ax + by + cz = d$.
3. 5 marins se retrouvent sur une île déserte. Ils ramassent le maximum de noix de coco. La nuit venue le premier décide de dissimuler sa part : il divise le tas en 5 parts égales, il reste une noix de coco qu'il jette, il cache sa part. Ainsi fait le second un peu plus tard, puis le troisième, le quatrième et le cinquième. Le lendemain ils se partagent le tas restant en 5 parts égales. Combien y-avait-il de noix de coco au départ ?

Exercice 3 - *Calculs dans* $\mathbb{Z}/n\mathbb{Z}$.

1. Rappeler le théorème des restes chinois et expliciter l'isomorphisme dans les deux sens.
2. Quelles sont les solutions d'une équation de la forme $ax \equiv b \mod n$?
3. Comment calculer un inverse, lorsqu'il existe ?

Exercice 4 - *Extensions algébriques.*

1. Soit k un corps commutatif et $P \in k[X]$. Décrire la structure d'anneau du quotient $k[X]/(P)$. Si $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{C}$, comment calcule-t-on dans l'extension algébrique $\mathbb{Q}(\alpha)$ de $\mathbb{Q}$?
2. Soit p un nombre premier et $F \in (\mathbb{Z}/p\mathbb{Z})[X]$ un polynôme irréductible de degré k. Montrer que $(\mathbb{Z}/p\mathbb{Z})[X]/(F)$ est un corps fini à p^k éléments (noté $\mathrm{GF}(p^k)$: rappelons que deux tels corps sont isomorphes !).

Exercice 5 - *Approximations de Padé.*
Soit f une fonction de classe C^∞ définie dans un voisinage de 0. On dit que $F = \frac{P}{Q} \in \mathbb{R}(X)$ est une *approximation de Padé* de type $[p/q]$ de f en 0 si : $\deg(P) \leq p$, $\deg(Q) \leq q$, $Q(0) = 1$, $f(x) - \frac{P(x)}{Q(x)} = O(x^{p+q})$. Expliquer comment l'algorithme d'Euclide permet de construire des approximations de Padé de f à partir de son développement de Taylor à l'origine.