UPMC PARIS UNIVERSITAS

# Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB
# Projet

Version du 16 octobre 2015

Le but du projet est d'implanter en C un programme permettant de résoudre un système de deux équations à deux inconnues $P, Q \in \mathbb{Z}[x, y]$. Pour cela, une borne sur la taille des solutions cherchées sera donnée en entrée.

L'algorithme devra utiliser le théorème des restes chinois pour faire les calculs modulo un nombre $p$ puis remonter les solutions dans $\mathbb{Z}$. La bibliothèque GMP sera utilisée pour l'arithmétique entière dépassant les capacités d'un mot-machine.

## Exercice 1 – Résultant

Une fois modulo $p$, la méthode suivante sera utilisée :

1. Calculer le résultant $R$ de $P, Q$ en $y$.
2. Déterminer les racines de $R$ modulo $p$. On pourra pour cela calculer le pgcd de $R$ et $x^p - x$ puis faire une recherche exhaustive.
3. En déduire les solutions du système modulo $p$.

## Exercice 2 – Sous-résultants

Cette méthode suppose que pour $x_0$ fixé, si $y_0$ et $y_1$ sont tels que $(x_0, y_0)$ et $(x_0, y_1)$ sont solutions, alors $y_0 = y_1$.

1. Effectuer un changement de variables linéaires sur les polynômes pour qu'avec grande probabilité, le système soit dans l'hypothèse supposée.
2. Calculer la suite $(R_i)_{0 \le i \le m,n}$ des sous-résultants de $P$ et $Q$. Notons $m$ le degré de $P$ en $y$ et $n$ celui de $Q$ en $y$. La sous-matrice $T_i$ de la matrice de Sylvester de $P$ et $Q$ est obtenue en retirant les $i$ dernières lignes de 0 de la sous-matrice construite à l'aide des colonnes 1 à $n-i$ et $n+1$ à $m+n-i$.

   Enfin, considérons la matrice $V_i$ de taille $(m+n-2i) \times (m+n-i)$. Le premier bloc de taille $m+n-2i-1$ est un bloc identité. Ensuite la dernière ligne est une ligne de $m+n-2i-1$ zéros (sous le bloc identité donc) suivis des coefficients $y^i, y^{i-1}, \ldots, 1$. Enfin, $R_i$ est le déterminant de $V_i\, T_i$. Le 0-ième sous-résultant doit être le résultant et de manière générale, le $i$-ième sous-résultant est un polynôme en $y$ de degré au plus $i$ à coefficients des polynômes en $x$.
3. Résoudre en $x$ le résultant $R = R_0$.
4. Pour $i$ de 1 à $\min(m, n)$, si $R_i(x_0, y)$ est non nul pour $x_0$ solution de $R$, alors déterminer $y$ et s'arrêter.
5. Accéler l'étape du calcul des solutions en $y$ en utilisant le fait que $R_i(x_0)(y)$ n'a pas de solution si et seulement si $x_0$ est racine du pgcd de $R_0$ et du coefficient de tête de $R_i$.