Formalisation de l'algorithme du PGCD rapide

Bruno Grenet et David Delahaye

LIRMM, Montpellier

Le calcul de PGCD est une brique de base en calcul mathématique effectif, entre autres utilisé pour l'inversion modulaire. Il est aussi l'objet d'un des plus anciens algorithmes formellement décrit, l'algorithme d'Euclide. Il existe d'autres algorithmes, plus rapides, pour ce problème, dont l'algorithme dit du « demi-PGCD ».

Cet algorithme est assez subtil, en particulier dans le cas des entiers, et de nombreuses preuves de la littérature comportent des erreurs. L'objectif de ce stage est de proposer une formalisation de la preuve de correction de cet algorithme dans l'assistant de preuve Coq, au moins dans le cas plus simple des polynômes.

Le stagiaire devra d'une part se familiariser avec Coq (s'il n'en est pas déjà familier) et étudier l'algorithme de demi-PGCD ainsi qu'une preuve relativement simple fournie par l'un des encadrants. Ensuite, l'objectif sera de formaliser cette preuve dans Coq. Une première étape pourra consister en la formalisation, bien plus simple, de l'algorithme d'Euclide.