
TD 2 : PGCD et inversion modulaire

Exercice 1.*Preuves manquantes*

1. Prouver que $a \equiv b \pmod{m} \Leftrightarrow (a \bmod m) = (b \bmod m)$
2. Prouver que si $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}^*$ et $*$ $\in \{+, -, \times\}$ alors

$$a \equiv b \pmod{m} \Rightarrow a * c \equiv b * c \pmod{m}$$

Exercice 2.*Vérification de la multiplication*

Pour vérifier que $489 * 542 = 265038$, on somme les chiffres de 489, ce qui donne 21, puis 3 quand on resomme les chiffres. On procède de même pour 542, ce qui donne 2. On multiplie $2 \cdot 3 = 6$. Puis on vérifie que cela correspond au même procédé pour le produit $265038 \rightsquigarrow 24 \rightsquigarrow 6$.

1. Justifier ce procédé en utilisant l'arithmétique modulo 9.
2. Décrivez un procédé semblable basé sur l'arithmétique modulo 11.

Exercice 3.*Programmation*

Il est impératif de tester chaque fonction codée !

1. Coder la division euclidienne de deux nombres entiers écrit sur une base β quelconque. Implémentez au moins les versions naïve et recherche dichotomique pour la division avec petit quotient.
2.
 - i. Écrire une fonction d'exponentiation rapide, qui calcule $a^b \bmod N$.
 - ii. Comparer le temps de calcul de cette fonction avec l'utilisation des opérateurs Python `a**b % N` et expliquer.