Contrôle du 17 novembre 2011

La notation accordera la plus grande importance à la qualité de la rédaction.

Un exemple de crible quadratique

Le but de ce problème est de factoriser le nombre $N = 10001$ en utilisant le crible quadratique.

1 . Expliquez le principe de cette méthode de factorisation. Vous en détaillerez les principales étapes. Vous donnerez quelques éléments pour l'analyse de la complexité de cet algorithme. Vous expliquerez pourquoi cet algorithme est plus efficace que le crible de Dixon.

2 . Écrivez une congruence modulo N du type

$$(a+m)^2 \equiv u_2 a^2 + u_1 a + u_0 \bmod N$$

dépendant d'un paramètre entier a. Ici m, u_0, u_1, u_2 sont des constantes entières bien choisies.

3 . Cherchez des valeurs de a comprises entre -6 et 6 qui permettent d'obtenir une congruence entre un carré et un nombre 5-friable modulo N. Vous expliquerez comment utiliser un crible, c'est-à-dire un tableau contenant toutes les valeurs de a. Vous illustrerez en détail l'utilisation de ce crible.

4 . Que se passe-t-il pour le nombre premier 2 ? Comment détecter les valeurs de $u_2a^2+u_1a+u_0$ qui sont divisibles par 4 ? par 8 ? par 16 ? par 32 ?

5 . Que se passe-t-il pour le nombre premier 3 ? Pourquoi ?

6 . Écrivez proprement toutes les congruences intéressantes obtenues. Portez les signes et les valuations dans une matrice M à coefficients entiers.

7 . Calculez le noyau de la réduction modulo 2 de la matrice M. Donnez la dimension de ce noyau, ainsi qu'une base.

8 . Pour chaque élément de cette base écrivez une congruence entre deux carrés modulo N. En déduire une factorisation (éventuellement triviale) de N.

9 . Complétez votre réponse à la première question.