

Feuille de travaux pratiques N°1

Nombres premiers et sommes de carrés

☞ Vous avez vu en cours que si p est un nombre premier de la forme $4k + 1$, alors il s'écrit comme somme de deux carrés. Le but de ce travail est de mettre en oeuvre un algorithme pour trouver de manière efficace une telle décomposition. Nous vous encourageons à passer du temps à bien comprendre la stratégie. Il sera sans doute nécessaire de charger le paquetage `numtheory` de Maple (i.e., faire `with(numtheory)` ; au début de votre session).

La stratégie

On va utiliser l'anneau $\mathbb{Z}[i]$ (avec i tel que $i^2 = -1$) et sa norme. Rappelons que si $x = a + bi$ est un élément de $\mathbb{Z}[i]$ alors on définit sa norme par $N(x) = a^2 + b^2$. Ce dernier élément est donc un entier positif. D'un autre côté, l'anneau $\mathbb{Z}[i]$ est principal. Donc tout idéal premier est principal, et accessoirement les idéaux premiers non-nuls sont maximaux. Un générateur d'un idéal premier est un élément premier de $\mathbb{Z}[i]$ et vous avez vu que si $N(x)$ est un nombre premier alors x est premier dans $\mathbb{Z}[i]$. Par exemple si $x = 1 + i$, $N(x) = 2$ et c'est donc un élément premier. Nous allons associer à un nombre premier p (de la forme $4k + 1$) un élément premier x_p de $\mathbb{Z}[i]$ tel que $N(x_p) = p$. Pour cela, nous allons faire apparaître x_p comme un générateur d'un idéal premier \mathfrak{p} de $\mathbb{Z}[i]$. Pour construire un tel idéal, on le réalise comme le noyau d'un morphisme d'anneau $f : \mathbb{Z}[i] \rightarrow \mathbb{F}_p$ (rappelons que pour nous $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$). En effet, puisque \mathbb{F}_p est un corps (donc intègre), le noyau de ce morphisme d'anneau sera un idéal maximal (donc premier). Un tel morphisme est entièrement caractérisé par l'image de 1 et de i . Néanmoins, étant un morphisme d'anneau, nous avons nécessairement $f(1) = 1$, et par suite ce morphisme est déterminé par $f(i)$. Or, i est un élément d'ordre 4 dans $\mathbb{Z}[i]^\times$. Il ne peut donc s'envoyer que sur un élément d'ordre 4 de \mathbb{F}_p^\times . Ensuite, on obtiendra notre générateur par «l'algorithme euclidien de $\mathbb{Z}[i]$ ».

Cela permet de mettre en évidence les deux ingrédients techniques dont nous aurons besoin :

- la division euclidienne dans $\mathbb{Z}[i]$,
- trouver un élément d'ordre 4 dans $\mathbb{Z}/p\mathbb{Z}$, p étant un nombre premier de la forme $4k + 1$.

Division euclidienne dans $\mathbb{Z}[i]$

- 1 Écrire une procédure `znorm` qui calcul la norme d'un élément de $\mathbb{Z}[i]$.
- 2 Écrire une division euclidienne dans $\mathbb{Z}[i]$ qui sera représenté par une fonction `zdiv` prenant en entrée deux éléments de $\mathbb{Z}[i]$ (on verra les éléments comme des nombres complexes) et qui renvoie un vecteur à deux élément représentant respectivement le quotient et le reste de la division euclidienne. Tester votre procédure sur les couples $(7 + i, 4 + 3i)$ et $(4 + 3i, 1 + i)$.

- 3** En mimant l'algorithme classique du pgcd, écrire une procédure `zgcd` qui renvoie le pgcd de deux éléments de $\mathbb{Z}[i]$.
- 4** Donner une condition nécessaire et suffisante pour qu'un élément de $\mathbb{Z}[i]$ soit premier et écrire une procédure `iszprime` renvoyant *true* si l'entier de Gauss donné est premier et *false* sinon. A l'aide de vos procédures, donner (aux inversibles près) la liste de tous les éléments premiers de $\mathbb{Z}[i]$ de norme ≤ 25 . En déduire la factorisation des éléments $7 + i$, $4 + 3i$, $5 + 3i$ et $7 + 2i$.

Élément d'ordre 4 dans $\mathbb{Z}/p\mathbb{Z}$

La stratégie est la suivante : si p est un nombre premier de la forme $4k + 1$, alors en prenant «au hasard» un élément a de \mathbb{F}_p^\times , il y a de «grande chance» que a^k soit un élément d'ordre 4.

- 5** Tester expérimentalement la stratégie proposée en prenant («au hasard») des $p \leq 1000$ de la forme désirée.

Remarque technique : pour tirer des nombres «au hasard» on pourra utiliser la fonction

```
RandomTools[Generate](integer(range=m..n))
```

qui renvoie un nombre entre deux entiers m et n . Par exemple la procédure suivante renvoie un nombre premier pseudo-aléatoire compris entre 3 et n ;

```
> randprime:=proc(n);
  RETURN(prevprime(RandomTools[Generate](integer(range=5..n+1))));
end;
```

- 6** A partir de vos tests, combien de a faut-il choisir en moyenne pour être sur d'en avoir un «bon». Donner des arguments théoriques pour valider vos résultats expérimentaux.
- 7** En déduire une procédure `ordre4` qui étant donné en entrée un nombre premier p de la forme $4k + 1$, renvoie un entier c , avec $|c| < p/2$, et tel que sa classe dans \mathbb{F}_p soit un élément d'ordre 4.

Décomposition de p en somme de deux carrés

- 8** Soit c un élément de \mathbb{Z} , tel que $|c| < p/2$ et sa classe modulo p soit d'ordre 4 dans \mathbb{F}_p^\times . On considère le morphisme d'anneau $f : \mathbb{Z}[i] \rightarrow \mathbb{F}_p$ défini par $f(1) = 1$ et $f(i) = c \pmod p$. Vérifier que c'est bien un morphisme d'anneau. Montrer que le noyau de f est engendré (en tant que \mathbb{Z} -module) par p et $i - c$. En déduire, par l'algorithme d'Euclide (dans $\mathbb{Z}[i]$), un générateur du noyau de f . Que doit-on prendre comme entiers a et b de façon à avoir $p = a^2 + b^2$?
- 9** En combinant l'ensemble de votre travail précédent, écrire une procédure `DeuxCarres`, qui prend en entrée un nombre premier p et qui renvoie un couple (a, b) tel que $p = a^2 + b^2$ si p est de la forme $4k + 1$.