Les nombres premiers 59 et 61 peuvent-ils s'écrire comme somme de deux carrés ? Le but de l'exercice est de montrer que les nombres premiers qui peuvent s'écrire comme somme de deux carrés (d'entiers relatifs) sont exactement ceux qui sont congrus à 1 modulo 4.

1. Soit p un nombre premier. Montrer par des congruences que si p est somme de deux carrés alors $p = 2$ ou $p = 1[4]$.

2. Soit $p = a^2 + b^2$ un nombre premier, $p \neq 2$, somme des deux carrés a^2 et b^2 des entiers a et b. Montrer que a et b sont inversibles modulo p et déterminer un élément d'ordre 4 dans le groupe multiplicatif des inversibles de $\mathbb{Z}/p\mathbb{Z}$. En déduire que 4 divise $p-1$.

3. Effectuer la division euclidienne dans $\mathbb{Z}[i]$ de 97 par $22+i$.

4. Dans toute la suite p est un nombre premier congru à 1 modulo 4. Nous cherchons à l'écrire comme somme de deux carrés, c'est à dire comme la norme d'un entier de Gauss. Montrer qu'il existe c une racine carré de -1 modulo p.

5. Supposons d'abord que $p = a_0^2 + b_0^2$. Calculer $(a_0 + cb_0)(a_0 - cb_0)[p]$. Il est donc naturel de considérer l'application

$$\begin{array}{rcl} \Phi \ : \ \mathbb{Z}[i] & \to & \mathbb{F}_p \\ (a+ib) & \mapsto & [a-cb]_p \end{array}$$

   Montrer que Φ est un morphime d'anneaux. Montrer que son noyau est un idéal principal. On notera g un de ces générateurs. Déterminer la norme de g.

6. Nous ne supposons désormais plus l'existence d'une écriture $p = a_0^2 + b_0^2$. Montrer que le noyau de l'application

$$\begin{array}{rcl} \Phi \ : \ \mathbb{Z}[i] & \to & \mathbb{F}_p \\ (a+ib) & \mapsto & [a-cb]_p \end{array}$$

   est l'idéal engendré par p et $c+i$. Montrer que le $pgcd(p, c+i)$ est un entier de Gauss de norme p.

7. Pour déterminer une racine de -1 modulo p, on écrit $p - 1 = 2^n m$ où m est un entier impair. Si x est un élément de $\mathbb{F}_p^\times$, $(x^m)^{2^n} = x^{p-1} = 1[p]$ par le petit théorème de Fermat. Par conséquent l'ordre de $y = x^m$ divise 2^n. Si cet ordre 2^k n'est pas 2, $y^{2^{k-2}} = y^{\frac{2^k}{4}}$ est un élément d'ordre 4. En pratique, on choisi un x au hasard, on calcule $y = x^m$ et si $y \neq 1[p]$ et $y \neq -1[p]$, on pose

$$\begin{array}{rcl} y_1 & = & y^2 \\ y_2 & = & y_1^2 \\ & \vdots & \\ y_{k-1} & = & (y_{k-2})^2 \ = \ y^{2^{k-1}} = -1 \\ y_k & = & (y_{k-1})^2 \ = \ y^{2^k} = 1 \end{array}$$

   L'entier c d'ordre 4 cherché peut être choisi comme y_{k-2}. Déterminer une racine de -1 modulo 97.

8. Écrire 97 comme somme de deux carrés.