Cercles en Arithmétique
Séance Parimaths du 12 novembre 2022

Louis Mallet-Burgues

1 Introduction

Ce document comporte les notes de la séance sur l'équation $x^2 + y^2 = c$. Il ne comporte pas tous les détails, y compris les figures. En revanche il y a aussi des choses non traitées pendant la séance par manque de temps. La dernière section regroupe des exercices et des indications (certains ont été posés et résolus, d'autres non).

On souhaite étudier les équations du type (E) : $x^2 + y^2 = c$ d'inconnues x et y et de paramètre c dans différents contextes arithmétiques.
Cas réel : quel est l'ensemble des solutions $(x, y) \in \mathbb{R}^2$ de l'équation (E) en fonction du paramètre $c \in \mathbb{R}$?

2 Cas rationnel

On sait très bien décrire l'ensemble des solutions dans le cas réel. Que se passe-t-il maintenant si $c = 1$ et si on cherche les solutions $(x, y) \in \mathbb{Q}^2$? Combien ya-t-il de solutions ? Reformulons la question géométriquement : combien ya-t-il de points à coordonnées rationnelles sur le cercle trigonométrique ?

Il y a 4 points évidents : $(-1, 0)$,$(1, 0)$,$(0, -1)$, d'autres moins évidents : $3^2 + 4^2 = 5^2$ donc $(3/5)^2 + (4/5)^2 = 1$.

Pour en trouver d'autres, on peut penser au paramétrage $(\cos\theta, \sin\theta)$ du cercle trigonométrique, mais on n'a aucune garantie que $\cos\theta$ et $\sin\theta$ vont être "souvent" rationnels. Il faut trouver un autre paramétrage : avec un dessin on peut avoir l'idée de poser $t = \tan\frac{\theta}{2}$ de sorte que :

$$(\cos\theta, \sin\theta) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$$

et

$$t = \frac{\sin\theta}{1+\cos\theta}$$

pour $\theta \in]-\pi, \pi[$. On pose alors $f(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ et on se convainc facilement que f est une bijection de $\mathbb{R}$ vers le cercle $\mathbb{U}$ privé de $(-1, 0)$. De plus :

$$t \in \mathbb{Q} \iff f(t) \in \mathbb{Q}^2$$

Le sens $\implies$ est immédiat, et l'autre sens vient du fait que $t = \frac{y}{1+x}$ si $f(t) = (x, y)$.
On peut alors restreindre f à $\mathbb{Q}$ et obtenir une bijection de $\mathbb{Q}$ dans l'ensemble des points rationnels de $\mathbb{U}$ privé de $(-1, 0)$: en particulier, il y a une infinité de points rationnels, et on les a tous trouvés ! Ce sont les $f(t)$ pour $t \in \mathbb{Q}$ ainsi que le point $(-1, 0)$.

Pour l'équation $x^2 + y^2 = r^2$ avec $r \in \mathbb{Q} \setminus \{0\}$, on peut se ramener à la précédente en divisant de chaque côté par r^2, et il y a donc aussi une infinité de solutions. Le cas où c n'est pas un carré de rationnel est plus délicat, et ne sera pas traité ici.

3 Cas entier

On veut maintenant étudier l'équation $x^2 + y^2 = c$ avec c un paramètre entier positif et x, y des inconnues entières. On ne va pas chercher à énumérer toutes les solutions en fonction du paramètre c (c'est possible mais délicat), mais on va plutôt chercher à quelle condition sur c il existe une solution.

3.1 Carrés modulo p

Définition. Soit $n \in \mathbb{N}^*$. On regroupe les entiers relatifs dans des paquets selon leur congruence modulo n (si $n = 8$ par exemple, on a un paquet qui contient $\ldots, -16, -8, 0, 8, 16, \ldots$, un paquet qui contient $\ldots, -15, -7, 1, 9, 17, \ldots$ etc.). On définit, pour n un entier positif, $\mathbb{Z}/n\mathbb{Z}$ comme l'ensemble de ces paquets, et on notera, pour $k \in \mathbb{Z}$, $\overline{k}$ le paquet auquel k appartient. On peut alors lister les éléments de $\mathbb{Z}/n\mathbb{Z}$:

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}$$

Il y en a exactement n. On peut ensuite définir une addition et une multiplication sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$, grâce à la propriété suivante :
Si $a \equiv a'$ et $b \equiv b'$ modulo n, alors $a + b \equiv a' + b'$ et $ab \equiv a'b'$ modulo n. Ainsi, il n'y a pas d'ambiguïté à poser $\overline{a} \times \overline{b} = \overline{ab}$ et $\overline{a} + \overline{b} = \overline{a+b}$.
On dit alors que $\mathbb{Z}/n\mathbb{Z}$, muni des opérations $+$ et $\times$ est un **anneau** (on gardera en tête que cela signifie qu'on peut y effectuer des additions, des multiplications, des soustractions, et qu'il y a un 0, ici $\overline{0}$ et un 1, ici $\overline{1}$).

Exemple de calcul dans $\mathbb{Z}/6\mathbb{Z}$:

$$\overline{5} \times \overline{14} + \overline{8} = \overline{5} \times \overline{2} + \overline{2} = \overline{12} = \overline{0}$$

Si p est un nombre premier, on peut également, en un sens, faire des divisions dans $\mathbb{Z}/p\mathbb{Z}$: en effet, si $\overline{a} \neq \overline{0}$ (autrement dit, $a \not\equiv 0$ modulo p), alors p et a sont premiers entre eux (car p est premier), donc il existe $u, v \in \mathbb{Z}$ tels que :

$$au + pv = 1$$

et donc, en réduisant modulo p :

$$\overline{au} = \overline{1}$$

et ainsi il existe un $\overline{u}$ inverse de $\overline{a}$ dans $\mathbb{Z}/p\mathbb{Z}$. Un tel élément est unique (dans $\mathbb{Z}/p\mathbb{Z}$, c'est à dire que u est unique modulo p), puisque si $\overline{va} = \overline{ua} = \overline{1}$, alors $p \mid a(u - v)$, or p et a sont premiers entre eux, donc par lemme de Gauss : $a \mid u - v$ et $\overline{u} = \overline{v}$.
Cet unique inverse sera alors noté $\overline{a}^{-1}$. Attention : ça n'a rien à voir avec $1/a$, l'inverse de a, qui n'est en général même pas un entier.

Exemple : l'inverse de $\overline{7}$ modulo 11 est $\overline{8}$ car $7 \times 8 \equiv 1$ modulo 11.
On fera attention, comme dans $\mathbb{R}$, à ne pas diviser par 0 : pour que $\overline{a}$ soit inversible modulo p, il faut quand même que $\overline{a} \neq \overline{0}$.

Puisqu'on peut faire des additions, des soustractions, des multiplications, et des divisions par un élément non nul, on dira que $\mathbb{Z}/p\mathbb{Z}$ est un **corps** (et on peut montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps exactement quand n est premier).

Exemple (modulo 7) :

$$\overline{3} \times \overline{5} + (\overline{6})^{-1} = \overline{1} + \overline{-1} = \overline{0}$$

À partir de maintenant et dans tout ce qui va suivre, on prendra :

$$\boxed{p \geq 3}$$

Proposition. Il y a exactement $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$ (un carré est un élément de la forme $\overline{a}^2$).

Démonstration. On considère E l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$, et on va ranger les éléments de $\mathbb{Z}/p\mathbb{Z}$ par paquets : on groupe $\overline{x}$ et $-\overline{x}$ ensemble. On remarque que $\overline{0}$ est tout seul dans son paquet, et c'est le seul élément à être tout seul dans son paquet : si $\overline{x}$ est seul dans son paquet, alors $x \equiv -x$ modulo p donc $p \mid 2x$, or p est impair donc $p \mid x$ et $\overline{x} = 0$. Or il y

a autant de paquets que d'éléments de E, puisque deux éléments ont le même carré si et seulement si ils sont dans le même paquet :

$$x^2 \equiv y^2 \iff p \mid (x-y)(x+y) \iff p \mid x-y \text{ ou } p \mid x+y \iff x \equiv \pm y$$

car p est premier. On a donc bien une correspondance bijective entre les éléments de E et les paquets. Il suffit donc de compter le nombre de paquets, notons le m. On a :

$$p = 2(m-1)+1$$

car il y a p éléments dans $\mathbb{Z}/p\mathbb{Z}$, et $m-1$ paquets à 2 éléments (ceux qui ne contiennent pas $\bar{0}$) et 1 paquet à un élément (celui qui contient $\bar{0}$ et rien d'autre). On a donc bien :

$$\boxed{m = \frac{p+1}{2}}$$

□

On peut faire mieux : on peut déterminer exactement quels éléments sont des carrés. Pour cela, on va admettre un résultat sur les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$: **un polynôme de degré n à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ a au plus n racines** (ce résultat est valable du fait que p est premier, et donc que $\mathbb{Z}/p\mathbb{Z}$ est un corps, ce qui permet de définir une division euclidienne sur les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, et on utilise cette division euclidienne pour aboutir au résultat). Noter que le résultat est bien connu si on remplace $\mathbb{R}$ par $\mathbb{Z}/p\mathbb{Z}$, et la même démonstration fonctionne, grâce au fait qu'on peut faire des divisions aussi dans $\mathbb{Z}/p\mathbb{Z}$.

Théorème. (Carrés modulo p)
Soit $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ différent de $\bar{0}$ (on dira non nul par la suite). On a alors :

$$\bar{x} \text{ est un carré modulo } p \iff \bar{x}^{\frac{p-1}{2}} = \bar{1}$$

Démonstration. Si $\bar{x}$ est un carré modulo p, alors on peut écrire $\bar{x} = \bar{y}^2$ pour un certain $\bar{y} \in \mathbb{Z}/p\mathbb{Z}$, et ainsi :

$$x^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1$$

modulo p par le petit théorème de Fermat, puisque p est premier avec y (si $p \mid y$, alors $p \mid x$, et c'est exclu).

Ceci montre que les carrés modulo p non nuls sont tous racines du polynôme $X^{\frac{p-1}{2}} - \bar{1}$ à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, or il y en a $\frac{p+1}{2} - 1 = \frac{p-1}{2}$, et ce polynôme a au plus $\frac{p-1}{2}$ racines, donc on conclut que les racines de ce polynôme sont exactement les carrés modulo p. □

Exemple. *À quelle condition sur p (premier impair), -1 est-il un carré modulo p ?*

D'après le théorème précédent, la condition équivaut à :

$$(-1)^{\frac{p-1}{2}} \equiv 1 \iff (-1)^{\frac{p-1}{2}} = 1$$

(car $p \geq 2$), et ceci est équivalent à :

$$p \equiv 1 \ [4]$$

3.2 Anneau des entiers de Gauss

Définition. On note $\mathbb{Z}[i]$ l'ensemble des **entiers de Gauss**, c'est à dire l'ensemble des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbb{Z}$. Géométriquement, cela forme un quadrillage de $\mathbb{C}$. Il est facile de vérifier que $\mathbb{Z}[i]$ est stable par addition, multiplication, soustraction et conjugaison complexe. C'est encore un anneau. En revanche, ce n'est pas un corps, car 2 n'a pas d'inverse dans $\mathbb{Z}[i]$ (ce serait nécessairement $1/2$ et $1/2 \notin \mathbb{Z}[i]$).

On dira qu'un élément $z \in \mathbb{Z}[i]$ est **inversible** dans $\mathbb{Z}[i]$ si il admet un inverse pour la multiplication dans $\mathbb{Z}[i]$, ce qui équivaut à dire que $z \neq 0$ et $1/z \in \mathbb{Z}[i]$. On dira enfin que $z \in \mathbb{Z}[i]$ est **irréductible** si il est non nul, non inversible et si on ne peut pas l'écrire comme un produit $z = ab$ avec $a, b \in \mathbb{Z}[i]$ non inversibles. C'est l'analogue sur $\mathbb{Z}[i]$ de la notion de nombre premier.

Pour éclaircir tout ça, déterminons tous les inversibles de $\mathbb{Z}[i]$. Des exemples d'inversibles sont $1, -1, i$ et $-i$, et pour voir que ce sont en fait les seuls, on va considérer la **norme** d'un élément $z \in \mathbb{Z}[i]$, définie par $N(z) = z\bar{z} = |z|^2$. Une première remarque est que $N(z) \in \mathbb{N}$, puisque z s'écrit $a + ib$ avec a et b dans $\mathbb{Z}$ et donc :

$$N(z) = a^2 + b^2 \in \mathbb{Z}$$

Ensuite, on a pour tous $a, b \in \mathbb{Z}[i]$, $N(ab) = N(a)N(b)$. De plus, si z est inversible, alors $N(z)N(1/z) = N(1) = 1$, or z et $1/z$ sont des entiers de Gauss donc leur norme est un entier, or si le produit de deux entiers naturels vaut 1, ces entiers valent tous les deux 1, donc $N(z) = 1$. Réciproquement, si $N(z) = 1$, alors $z\bar{z} = 1$, or $\bar{z} \in \mathbb{Z}[i]$ donc z est inversible. Au final on a :

$$\boxed{z \text{ inversible } \iff N(z) = 1}$$

Et il est très facile, par un dessin (ou par un calcul) de voir que les seuls entiers de Gauss de norme 1 (c'est à dire de module 1) sont $1, -1, i$ et $-i$.

Théorème. (Division euclidienne dans $\mathbb{Z}[i]$)
Soient $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. Il existe $q, r \in \mathbb{Z}[i]$ tels que :

$$\begin{cases} a = bq + r \\ N(r) < N(b) \end{cases}$$

Cet énoncé ressemble beaucoup à celui de la division euclidienne sur $\mathbb{Z}$, sauf qu'on n'assure pas l'unicité du couple (q, r). On dit d'ailleurs que $\mathbb{Z}[i]$ est un **anneau euclidien**.

Démonstration. Considérons $z = a/b \in \mathbb{C}$. Ce n'est à priori pas un entier de Gauss, mais c'est un nombre complexe ($b \neq 0$). Par un dessin de la grille que forme $\mathbb{Z}[i]$ dans le plan $\mathbb{C}$, on voit que l'entier de Gauss q le plus proche de z est à une distance au plus $\sqrt{2}/2$ de z. On a donc $|z - q| \leq \sqrt{2}/2$. On multiplie alors cette inégalité par $|b|$, et on obtient :

$$|a - bq| \leq \sqrt{2}/2\,|b|$$

On pose alors $r = a - bq \in \mathbb{Z}[i]$ car $\mathbb{Z}[i]$ est stable par soustraction et multiplication. On a donc, en mettant l'inégalité précédente au carré :

$$N(r) \leq \frac{1}{2}N(b)$$

et en particulier $N(r) < N(b)$: c'est ce qu'on voulait. □

On a besoin d'un dernier résultat un peu technique (une sorte de lemme de Gauss pour les éléments irréductibles) pour pouvoir continuer. La démonstration donnée peut sembler compliquée (elle adapte des outils théoriques avec lesquels elle serait beaucoup plus claire, mais l'objet n'est pas ici de faire un cours sur les anneaux). On peut bien sûr admettre le résultat pour la suite.

Lemme. Soit $a \in \mathbb{Z}[i]$ irréductible et $b, c \in \mathbb{Z}[i]$ tels que $a \mid bc$. Alors $a \mid b$ ou $a \mid c$. (Ici, $a \mid b$ signifie qu'il existe $k \in \mathbb{Z}[i]$ tel que $b = ka$.)

Démonstration. On considère pour cela $A = \{\lambda a + \mu b \mid \lambda, \mu \in \mathbb{Z}[i]\}$ et on vérifie facilement que A est un **idéal** de $\mathbb{Z}[i]$, c'est à dire qu'il est stable par $+$, par $-$, il contient 0 et pour tout $x \in A$ et $z \in \mathbb{Z}[i]$, le produit xz est encore dans A.

A ne contient pas que 0 puisque $a \neq 0$ et $a \in A$. Il existe donc un élément $x \in A$ non nul de **norme minimale** parmi les éléments non nuls de A (puisque la norme est un entier naturel, et toute partie non vide de $\mathbb{N}$ admet un minimum). Il est alors facile de vérifier que $x\mathbb{Z}[i]$ est contenu dans A (c'est à dire que tout produit xy avec $y \in \mathbb{Z}[i]$ est encore dans A). Montrons l'autre inclusion : si $u \in A$, on peut écrire la division euclidienne de u par x puisque x est non nul : il existe $q, r \in \mathbb{Z}[i]$ avec $N(r) < N(x)$ tels que :

$$u = qx + r$$

et donc $r = u - qx \in A$ puisque A est un idéal. On a alors $r = 0$, sinon x ne serait pas de norme minimale parmi les éléments non nuls de A. Donc $u = qx \in x\mathbb{Z}[i]$. Au total :

$$\boxed{A = x\mathbb{Z}[i]}$$

On a donc $x \mid a$ puisque $a \in A$, on peut donc écrire $a = xy$ avec $y \in \mathbb{Z}[i]$, et par irréductibilité de a, on a x inversible ou y inversible.
Si x est inversible, alors il n'est pas dur de voir que $A = \mathbb{Z}[i]$ et donc $1 \in A$, et donc il existe $\lambda, \mu \in \mathbb{Z}[i]$ tels que $1 = \lambda a + \mu b$. On a donc $c = \lambda ac + \mu bc$, or $a \mid bc$ donc $a \mid c$: on conclut dans ce cas.
Sinon, y est inversible, donc on vérifie aisément que $A = a\mathbb{Z}[i]$, or $b \in A$ donc $a \mid b$: on conclut aussi dans ce cas.

□

3.3 Entiers qui s'écrivent comme somme de deux carrés

On va ici déterminer tous les entiers qui s'écrivent comme somme de deux carrés d'entiers, c'est à dire les $c \in \mathbb{N}$ tels que l'équation $x^2 + y^2 = c$ admette une solution (avec x, y entiers). Pour cela, on commence par chercher quels sont les nombres premiers qui sont somme de deux carrés. On attribue à Gauss le résultat suivant :

Théorème. *(Gauss)* Soit p un nombre premier impair. Les propositions suivantes sont équivalentes :

1. p peut s'écrire comme la somme de deux carrés d'entiers
2. $p \equiv 1$ [4]
3. -1 est un carré modulo p
4. p n'est pas irréductible dans $\mathbb{Z}[i]$

Démonstration. **1 implique 3 :** Supposons (1) vrai, on peut donc écrire $p = x^2 + y^2$ avec $x, y \in \mathbb{Z}$, et en réduisant modulo p on obtient :

$$-x^2 \equiv y^2$$

modulo p. De plus, x n'est pas divisible par p : si $p \mid x$, alors $p \mid p - x^2$ donc $p \mid y^2$, or p est premier donc $p \mid y$, et ainsi $p^2 \mid x^2$ et $p^2 \mid y^2$ donc $p^2 \mid x^2 + y^2$ et $p^2 \mid p$: c'est impossible. (Ces relations de divisibilités ont lieu dans $\mathbb{Z}$, pas dans $\mathbb{Z}[i]$). Ainsi, x est inversible modulo p, et on obtient alors, en multipliant par $(\overline{x}^{-1})^2$:

$$-\bar{1} = (\bar{y} \times \bar{x}^{-1})^2$$

donc -1 est un carré modulo p.

3 implique 4 : Supposons (3) vrai, il existe alors $a \in \mathbb{Z}$ tel que $a^2 \equiv -1$ modulo p, donc $p \mid a^2 + 1$. Cette divisibilité a lieu dans $\mathbb{Z}$, donc aussi dans $\mathbb{Z}[i]$, et ainsi $p \mid (a + i)(a - i)$ dans l'anneau des entiers de Gauss. Supposons alors par l'absurde que p soit irréductible. Le lemme prouvé précédemment entraîne que $p \mid a + i$ ou $p \mid a - i$, et on se convainc facilement que c'est impossible (sinon on peut écrire $a + i = p\lambda + p\mu i$ et ainsi en identifiant les parties imaginaires on trouve que p divise 1 dans $\mathbb{Z}$, et c'est impossible). p n'est donc pas irréductible dans $\mathbb{Z}[i]$.

4 implique 1 : Supposons (4) vrai. p n'étant pas inversible dans $\mathbb{Z}[i]$ (ce n'est pas $1, -1, i, -i$), et n'étant pas non plus nul, son irréductibilité signifie qu'il existe $a, b \in \mathbb{Z}[i]$ non inversibles tels que :

$$p = ab$$

On passe à la norme :

$$N(p) = p^2 = N(a)N(b)$$

Or p est premier et $N(a), N(b)$ sont des entiers naturels donc il n'y a que trois possibilités : $N(a) = N(b) = p$ ou $N(a) = 1$, $N(b) = p$ ou $N(a) = p$, $N(b) = 1$. Mais a et b sont non inversibles donc leur norme ne vaut pas 1, et ainsi :

$$N(a) = p$$

Autrement dit, en notant $a = x + iy$ avec $x, y \in \mathbb{Z}$:

$$x^2 + y^2 = p$$

donc p est une somme de deux carrés.

Enfin, on a déjà montré dans la section sur les carrés modulo p que les points (2) et (3) étaient équivalents. □

On sait donc que les nombres premiers impairs qui s'écrivent comme somme de deux carrés sont exactement ceux qui sont congrus à 1 modulo 4. Essayons de déterminer à quelle condition un entier $n \geq 1$ peut s'écrire comme somme de deux carrés. On note C l'ensemble des nombres entiers de la forme $x^2 + y^2$ avec $x, y \in \mathbb{Z}$.

Ce qui suit n'a pas été traité pendant la séance.

Lemme. C est stable par multiplication.

Démonstration. Ce résultat n'est pas facile à démontrer sans aucune intuition géométrique (on peut essayer de retourner l'expression de $(a^2 + b^2)(c^2 + d^2)$ dans tous les sens pendant longtemps sans arriver à l'exprimer comme somme de deux carrés). Avec ce qu'on a fait cependant, le lemme est évident : C est exactement l'ensemble des $N(z)$ pour $z \in \mathbb{Z}[i]$, et donc si $N(z), N(z')$ sont deux éléments de C, leur produit $N(zz')$ est aussi un élément de C. □

Théorème. Un entier $n \geq 1$ est élément de C si et seulement si, pour tout nombre premier p congru à 3 modulo 4, la valuation p-adique de n est paire.

Démonstration. Supposons que pour tout nombre premier p congru à 3 modulo 4, la valuation p-adique de n est paire. On peut alors écrire la décomposition de n en produit de facteurs premiers, qui donne :

$$n = \left(\prod_{p \equiv 3 \ [4]} p^{v_p(n)} \right) \times \left(\prod_{p \equiv 1 \ [4]} p^{v_p(n)} \right) \times 2^{v_2(n)}$$

Le premier de ces trois facteurs est un carré parfait car les exposants qui y apparaissant sont pairs. Ensuite, le second facteur est dans C car pour tout p congru à 1 modulo 4, $p \in C$

(d'après le théorème de Gauss démontré précedemment), et C est stable par multiplication. De même, $2 \in C$ car $2 = 1^2 + 1^2$ donc $2^{v_2(n)} \in C$, et au total, puisque C est stable par produit :

$$\boxed{n \in C}$$

À présent, montrons par **récurrence forte** sur n que si n appartient à C, alors pour tout nombre premier p congru à 3 modulo 4, $v_p(n)$ est pair. Le cas $n = 1$ est immédiat car toutes les valuations p -adiques de 1 valent 0.
Supposons $n \geq 2$ et que le résultat est vrai aux rangs précédents. On veut montrer le résultat pour n, on suppose donc que n appartient à C. On peut écrire $n = a^2 + b^2$ avec a et b entiers. Soit p un nombre premier congru à 3 modulo 4. On veut montrer que $v_p(n)$ est pair. Si p ne divise pas n, le résultat est clair. Sinon, $p \mid a^2 + b^2$. Il y a alors deux cas à traiter : si p divise a et si p ne divise pas a. Si p divise a, on a aussi $p \mid b^2$ et donc $p \mid b$ et $p^2 \mid a^2 + b^2$ par combinaisons linéaires, et ainsi :

$$\frac{n}{p^2} = (a/p)^2 + (b/p)^2$$

est un entier qui s'écrit comme somme de deux carrés d'entiers, c'est donc un élément de C, et par hypothèse de récurrence, $v_p(n/p^2)$ est paire, donc :

$$v_p(n) = 2 + v_p(n/p^2)$$

est paire aussi. Si p ne divise pas a, alors a est inversible modulo p et donc, de $a^2 + b^2 \equiv 0$ modulo p, on déduit que -1 est un carré modulo p (en multipliant par le carré de l'inverse de a modulo p de chaque côté), mais ceci est impossible puisque $p \not\equiv 1$ [4] (et $p \neq 2$). Ceci achève la récurrence. □

4 Cas modulo p

Cette dernière section s'adresse plutôt à des élèves de première année après le bac.
On va, pour finir, regarder l'équation $x^2 + y^2 = c$ avec $c \in \mathbb{Z}/p\mathbb{Z}$ un paramètre et avec $x, y \in \mathbb{Z}/p\mathbb{Z}$ les inconnues. On va être en mesure de compter exactement le nombre de solutions pour chaque p et chaque c. **Dans toute la suite p est un nombre premier impair, et on notera directement x un élément de $\mathbb{Z}/p\mathbb{Z}$ plutôt que $\overline{a}$ avec $a \in \mathbb{Z}$.**

On notera $U_c = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid x^2 + y^2 = c\}$ l'ensemble des solutions de l'équation. On peut le voir comme une sorte de "cercle" du "plan" $(\mathbb{Z}/p\mathbb{Z})^2$.

4.1 Étude d'un exemple

Prenons $p = 5$ pour essayer de comprendre la situation. On peut se rendre compte à la main que les valeurs de $|U_c|$ (où $|U_c|$ désigne le nombre d'éléments de U_c) sont les suivantes :

c	$\lvert U_c\rvert$
0	9
1	4
2	4
3	4
4	4

On constate que pour $c \neq 0$, le nombre de solutions semble être toujours le même (d'ailleurs on peut vérifier que $9+4+4+4+4 = 25 = 5^2$ donc on n'a rien oublié).

En plus, on constate qu'il existe toujours au moins une solution (ce qui n'était pas le cas dans $\mathbb{Z}$). On va naturellement essayer de démontrer ces observations en toute généralité.

4.2 Existence de solutions et cas particuliers

Proposition. Pour tout $c \in \mathbb{Z}/p\mathbb{Z}$, U_c est non vide (il existe une solution).

Démonstration. J'avais pensé au départ à une preuve compliquée de ceci (utilisant trois fois le théorème de Lagrange). La preuve qui suit, bien plus élémentaire, m'a été proposée par un camarade (on remerciera donc Ferdinand pour sa preuve). On sait déjà que l'ensemble des de $\mathbb{Z}/p\mathbb{Z}$, noté E, possède $\frac{p+1}{2}$ éléments. Ainsi, puisque l'ensemble $-E+c$ a également $\frac{p+1}{2}$ éléments, et que $\frac{p+1}{2} + \frac{p+1}{2} > p$, les ensembles E et $-E+c$ s'intersectent, ils ont donc un élément x en commun, et d'une part $x \in E$ donc on peut écrire x sous la forme y^2 et d'autre part $x \in -E+c$ donc on peut écrire x sous la forme $-z^2+c$, et ainsi $y^2 = -z^2 + c$ donc :

$$\boxed{c = y^2 + z^2}$$

On a bien trouvé une solution. □

Il s'agit maintenant de déterminer le cardinal de U_c. On va commencer par des cas particuliers sympathiques qui permettent d'utiliser tout ce qu'on a vu jusqu'ici.

Proposition. U_1 possède $p-1$ éléments si $p \equiv 1\ [4]$ et $p+1$ éléments sinon.

Démonstration. Il s'agit ici de résoudre l'équation $x^2+y^2=1$. Pour cela, on utilise la même stratégie que dans le cas rationnel : on considère la fonction f qui à t associe :

$$f(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

où les divisions correspondent à des multiplications par l'inverse. $f(t)$ est alors bien définie si et seulement si t n'est pas une racine carrée de -1. On note alors A l'ensemble $\mathbb{Z}/p\mathbb{Z}$ privé des éventuelles racines carrées de -1 et B l'ensemble U_1 privé du point $(-1,0)$. On vérifie alors (comme dans le cas rationnel vu au tout début) que f réalise une bijection de A dans B. Ainsi, A et B ont autant d'éléments et donc :

$$|U_1| = 1 + |B| = 1 + |A|$$

Or si $p \equiv 1$ [4], -1 possède exactement deux racines carrées donc $|A| = p-2$ et finalement $|U_1| = p-1$. Enfin, si $p \equiv 3$ [4], -1 n'a aucune racine carrée (comme vu précedemment) donc $|A| = p$ et $|U_1| = p+1$. □

Un autre cas particulier où l'on sait donner le nombre d'éléments de U_c est lorsque $c = 0$ et $p \equiv 1$ [4].

Proposition. Si $p \equiv 1$ [4], alors $|U_0| = 2p-1$.

Démonstration. L'idée ici est que, p étant congru à 1 modulo 4, on dispose d'une racine carrée de -1, appelons là i pour l'analogie avec les nombres complexes. L'équation devient alors :

$$x^2 + y^2 = 0 \iff (x+iy)(x-iy) = 0 \iff x = \pm iy$$

car $\mathbb{Z}/p\mathbb{Z}$ est un corps. Il est alors très facile de dénombrer les solutions : en fixant $y \in \mathbb{Z}/p\mathbb{Z}$, le nombre de x égaux à $\pm iy$ est 2 si $y \neq 0$ (car p est impair) et 1 si $y = 0$. Il y a donc en tout :

$$2(p-1) + 1 = 2p - 1$$

solutions. □

4.3 En général

Voyons enfin le cas général, qui englobe les résultats précédents. On prend ici c quelconque dans $\mathbb{Z}/p\mathbb{Z}$.

Définition. Pour $a \in \mathbb{Z}/p\mathbb{Z}$, on va noter $\chi(a) = 1$ si a est un carré non nul, $\chi(A) = -1$ si a n'est pas un carré, et $\chi(a) = 0$ si $a = 0$. χ s'appelle le **symbole de Legendre** et est noté $\left(\frac{a}{p}\right)$ dans la littérature, notation que j'évite ici pour ne pas la confondre avec une fraction. Par exemple, si $p = 7$, $\chi(3) = -1$ et $\chi(4) = 1$. On a montré précedemment que :

$$\boxed{\chi(-1) = (-1)^{\frac{p-1}{2}}}$$

puisque -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4. La propriété fondamentale que l'on va utiliser est la suivante : pour tous $a, b \in \mathbb{Z}/p\mathbb{Z}$:

$$\boxed{\chi(ab) = \chi(a)\chi(b)}$$

Cela se vérifie sans difficulté.

On commence par une remarque facile : un élément $a \in \mathbb{Z}/p\mathbb{Z}$ possède **exactement** $1 + \chi(a)$ racines carrées dans $\mathbb{Z}/p\mathbb{Z}$. En effet, ou bien $a = 0$ et a possède une seule racine carrée, ou bien a est un carré non nul et a alors exactement deux racines carrées (car p est premier et impair), ou bien a n'est pas un carré et n'a alors pas de racines carrées.

Théorème. (Nombre de solutions modulo p pour c quelconque)

$$|U_c| = \begin{cases} p + (-1)^{\frac{p+1}{2}} & \text{si } c \neq 0 \\ p + (1-p)(-1)^{\frac{p+1}{2}} & \text{si } c = 0 \end{cases}$$

Démonstration. Voyons le cas $c \neq 0$. On a alors :

$$x^2 + y^2 = c \iff \frac{x^2}{c} + \frac{y^2}{c} = 1$$

Ainsi, en notant $u = \frac{x^2}{c}$ et $v = \frac{y^2}{c}$, on peut dénombrer $|U_c|$ en sommant sur toutes les valeurs possibles de u et v :

$$\begin{aligned} |U_c| &= \sum_{u+v=1} \left| \{x \in \mathbb{Z}/p\mathbb{Z} \mid \frac{x^2}{c} = u\} \right| \times \left| \{y \in \mathbb{Z}/p\mathbb{Z} \mid \frac{y^2}{c} = v\} \right| \\ &= \sum_{u+v=1} \left| \{x \in \mathbb{Z}/p\mathbb{Z} \mid x^2 = cu\} \right| \times \left| \{y \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = cv\} \right| \\ &= \sum_{u+v=1} (\text{nombre de racines carrées de } cu) \times (\text{nombre de racines carrées de } cv) \\ &= \sum_{u+v=1} (1 + \chi(cu))\,(1 + \chi(cv)) \\ &= \sum_{u+v=1} 1 + \sum_{u+v=1} \chi(cu) + \sum_{u+v=1} \chi(cv) + \sum_{u+v=1} \chi(cu)\chi(cv) \\ &= p + 2\chi(c) \sum_{u \in \mathbb{Z}/p\mathbb{Z}} \chi(u) + \chi(c)^2 \sum_{u+v=1} \chi(u)\chi(v) \end{aligned}$$

Remarquons de plus que $\sum_{u \in \mathbb{Z}/p\mathbb{Z}} \chi(u) = 0$ car il y a autant de carrés non nuls que de non-carrés (il y en a $\frac{p-1}{2}$). Ensuite, $\chi(c)^2 = (\pm 1)^2 = 1$. On a donc :

$$\boxed{|U_c| = p + \sum_{u+v=1} \chi(u)\chi(v)}$$

On a alors montré que $|U_c|$ **ne dépend pas de** c, comme conjecturé précedemment. Or on connait $|U_1|$ d'après ce qui précède ! (On pourrait aussi continuer le calcul en faisant un changement de variable assez astucieux du type $w = 1/v$ et en utilisant la bijectivité de $x \mapsto \frac{x}{1+x}$, mais c'est moins élégant). Ainsi :

$$|U_c| = |U_1| = p + (-1)^{\frac{p+1}{2}}$$

par une disjonction de cas facile entre les cas p congru à 1 ou 4 modulo p.

Enfin, pour le cas $c = 0$, il suffit de remarquer que :

$$p^2 = \sum_{c \in \mathbb{Z}/p\mathbb{Z}} |U_c|$$

puisque les cercles U_c partitionnent $(\mathbb{Z}/p\mathbb{Z})^2$. On a alors :

$$|U_0| = p^2 - (p-1)\left(p + (-1)^{\frac{p+1}{2}}\right) = p + (1-p)(-1)^{\frac{p+1}{2}}$$

comme annoncé. □

On est parvenu à dénombrer le cercle U_c en toute généralité (à part pour le cas $p = 2$ qui est sans intérêt). On pourra remarquer que le résultat général trouvé ici concorde avec le cas $p = 5$ étudié plus haut : c'est rassurant !

5 Exercices

Les exercices ne sont pas par ordre de difficulté, et ils n'ont pas tous été traités pendant la séance (le 4 et le 5 sont les plus abordables). Les exercices 1, 2, 4, 5 (sauf la dernière question) et 6 ont été traités pendant la séance.

Exercice 1. (Théorème de Wilson) Soit $n \geq 2$ un entier. Montrer que n est premier si et seulement si $(n-1)! \equiv -1\ [n]$.
Pour le sens direct, on pourra regrouper les éléments de $\mathbb{Z}/p\mathbb{Z}$ par paquets de 1 ou 2 éléments, en regroupant $\bar{x}$ avec son inverse modulo p.

Exercice 2. Soit p un nombre premier et $a, b, c \in \mathbb{Z}$ avec a non multiple de p. Montrer que l'équation $ax^2 + bx + c \equiv 0\ [p]$ admet une solution si et seulement si $\Delta = b^2 - 4ac$ est un carré modulo p. *On pourra passer par une forme canonique.*

Exercice 3. (Difficile) Résoudre l'équation :

$$x^{62} + x^{121} + 43 \equiv 0\ [77]$$

On pourra d'abord, à l'aide du théorème des restes chinois, montrer que si 7 et 11 ne sont pas des diviseurs de x, alors $x^{60} \equiv 1\ [77]$. On résoudra ensuite l'équation modulo 7 et 11 à l'aide de l'exercice qui précède avant de "recoller" les solutions par théorème des restes chinois encore une fois.

Exercice 4. Existe-t-il 1000 nombres entiers consécutifs non premiers ?

Exercice 5. -Montrer qu'il existe une infinité de nombres premiers.
-En adaptant la méthode utilisée, montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.
-En utilisant le critère $p \equiv 1\ [4]$ si et seulement si -1 est un carré modulo p, montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4. *On pourra considérer $n!^2 + 1$ et ses diviseurs premiers.*

Exercice 6. Soit $r \in \mathbb{N}$. On note A_r le nombre de solutions de **l'inéquation** $x^2 + y^2 \leq r^2$ (qui correspond au nombre de points à coordonnées entières dans le disque de centre $(0, 0)$ et de rayon r). Déterminer :

$$\lim_{r \longrightarrow +\infty} \frac{A_r}{r^2}$$

On pourra d'abord trouver un argument visuel puis le rendre rigoureux en calculant ce cardinal avec une imprécision majorée par une constante fois r, et en faisant apparaître une somme de Riemann.

Exercice 7. (Difficile) Déterminer le reste de $\Omega(n) = \prod_{1 \leq k \leq n,\ k \wedge n = 1} k$ modulo n. *Pour cela, on pourra regarder le cas où n est une puissance de p en adaptant l'idée de l'exercice* 1*, puis montrer que, si m et n sont premiers entre eux, $\Omega(mn) \equiv \Omega(m)^{\varphi(n)}\ [m]$ avec $\varphi(n)$ le nombre de nombres premiers avec n entre* 1 *et n.*