cercles modulo *p*

par M. Etienne Coulomb (TS), M. Sam Messavusu (TS), M. Stéphane Deblick (1°S), M. Nicolas Ferrey (1°S), M. Sébastien Serrant (1°S), élèves du **lycée Pablo Picasso de Fontenay sous bois (94)** et M. Yann Chauvin (TS), M. Lhocine Aliouane (1°S), M. Marc Bouvier (1°S), M. Arash Mostafa Zadeh (1°S), élèves du **lycée Romain Rolland d'Ivry (94)**

enseignants :
Mmes Monique Corlay, Claude Parreau
Mmes et M. Lise Bernigole, Jean-Paul Bernigole, Christiane Guedj

chercheur :
M. Olivier Piltant

coordination article : ALIOUANE Lhocine

niveau de lecture : ≥ classe de première

Pas de compte-rendu de parrainage.

[Avertissement : si vous n'avez aucune connaissance sur le langage des congruences dans Z, commencez par lire l'annexe 1 à la fin de cet article.]

NGa— Cercle $x^2 + y^2 = 1$ "modulo *p*" **4**

L'équation $x^2 + y^2 = 1$ (cercle de rayon 1) n'a que quatre solutions en nombres entiers. A-t-on plus de solutions lorsqu'on calcule modulo *p* (*p* étant un nombre premier fixé), c'est-à-dire en négligeant tout multiple de *p* et en ne retenant de chaque nombre que son reste après division par *p* ? Comment peut-on visualiser ces solutions et trouver un moyen de les compter ?

Le problème.

$x^2 + y^2 = 1$ est, dans un repère orthonormé, l'équation d'un cercle de centre (0, 0) et de rayon 1.

Il y a sur ce cercle quatre points particuliers : ils ont des coordonnées entières ; ce sont les points d'intersection avec les axes des abscisses et des ordonnées …

(0, 1) ; (0, –1) ; (1, 0) ; (–1, 0).

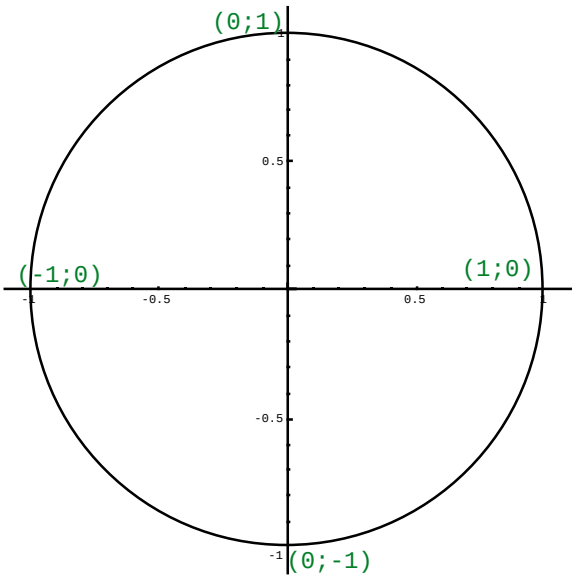

Figure 1

Maintenant, combien y a-t-il de solutions entières [NDLC : c'est-à-dire de points à coordonnées entières], si on se place à un multiple de *p* près (*p* étant un nombre premier, c'est-à-dire qu'il n'est divisible que par 1 et lui-même) ?

Premier traitement.

L'équation devient

$$x^2 + y^2 \equiv 1 \ [p], \quad \text{équation } \mathbf{(1)}$$

c'est-à-dire qu'il existe un entier *k* tel que

$$x^2 + y^2 = 1 + kp.$$

Position des solutions.

Si on trace de façon empirique l'ensemble des solutions de $x^2 + y^2 = 1 + kp$, k prenant toutes les valeurs dans Z (on peut se limiter à N car si $k < 0$, on a $x^2 + y^2 < 0$, qui n'a pas de solution), on obtient une série de cercles concentriques de rayons $\sqrt{(1 + kp)}$. On note alors graphiquement les solutions entières appartenant à l'un des cercles et on les relie.

On obtient alors les figures suivantes :

***p* = 5**

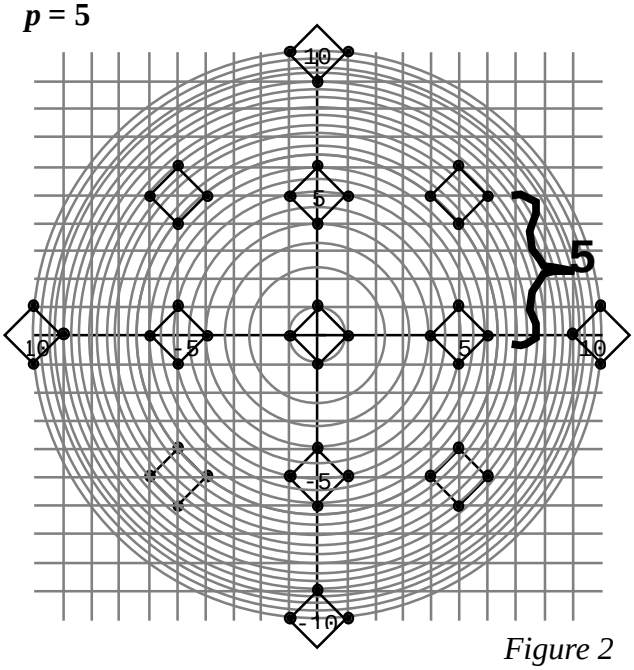

Figure 2

***p* = 7**

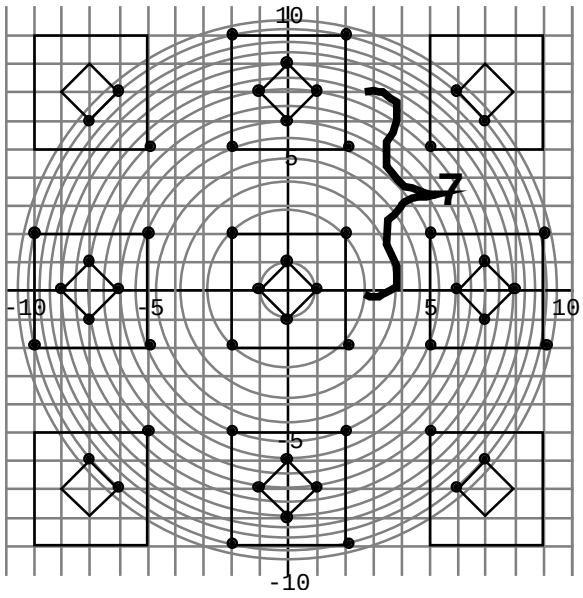

Figure 3

***p* = 11**

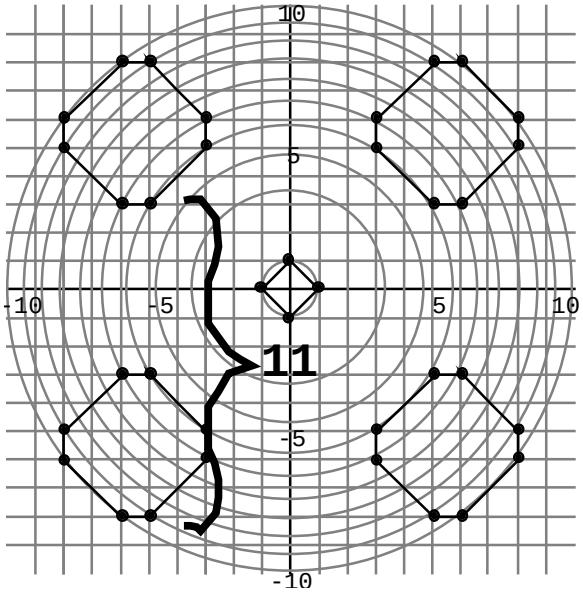

Figure 4

On remarque immédiatement que les solutions de $x^2 + y^2 \equiv 1\ [p]\ /\ (x,y) \in Z^2$ ne semblent pas être placées "au hasard" : une figure semble subir une translation de vecteur dont les coordonnées sont des multiples de *p*, par exemple

$$\vec{v}_1(3p,0)\ ;\ \vec{v}_2(p,p)$$

plus généralement de vecteur $\vec{v}(kp, k'p)$, $(k, k') \in Z^2$.

[NDLC : il semble que l'expression « figure semble subir une translation » doive être comprise comme « figure inchangée quand on lui fait subir […] une translation » ; préparez-vous à subir cette formulation.]

[NDLC : les illusions d'optique sont ce qu'elles sont, les segments sont des segments, si certains segments coupés par des cercles ont l'air d'être tordus … vérifiez qu'ils sont droits !]

Pour démontrer qu'une figure peut subir une de ces translations, il suffit de démontrer :

Théorème 1 :

Chaque solution après avoir subi une translation de vecteur $\vec{v}(kp, k'p)$***, reste une solution de l'équation*** (c'est-à-dire qu'elle est sur l'un des cercles).

Démonstration :

Soit $(x, y) \in \mathbb{Z}^2 / x^2 + y^2 \equiv 1 [p]$: (x, y) est donc une solution de l'équation. Soit (X, Y) les coordonnées du point issu de la translation de vecteur $\vec{v}(kp, k'p)$, on a alors :

$$\begin{cases} X = x + kp \\ Y = y + k'p \end{cases}$$

Le calcul de $X^2 + Y^2 \equiv 1 [p]$ (en fonction de x, y, k, k' et p) donne (on utilise le fait que $x^2 + y^2 \equiv 1 [p]$) :

$$X^2 + Y^2 = 1 + Kp [p]$$

où K est un entier. Donc :

$$X^2 + Y^2 \equiv 1 [p].$$

Applications :

1) On peut obtenir une infinité de solutions « à p près » à partir d'une solution :

(x, y) sera la même solution à p près que $(x + kp, y + k'p)$

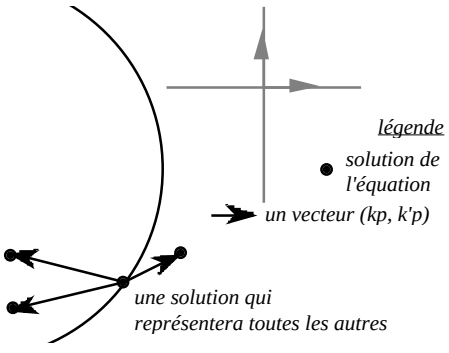

Figure 5

2) Si on connaît toutes les solutions dans un carré de côté p, à côtés parallèles aux axes, on connaît toutes les solutions de l'équation, car une solution hors du carré peut être « ramenée » dans le carré par la translation de vecteur $\vec{v}(kp, k'p)$.

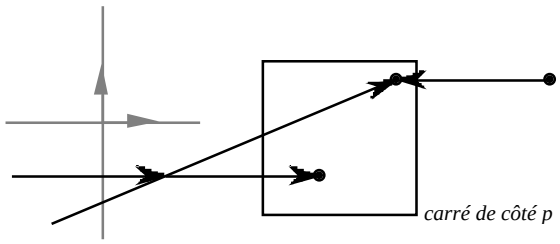

Figure 6

Remarques :

(*i*)— La démonstration ci-contre n'utilisant pas le fait que p soit un nombre premier, elle est encore valable si l'on choisit un nombre quelconque non premier : $m \in \mathbb{Z}$, au lieu de p premier.

Donc :

Pour l'équation $x^2 + y^2 \equiv 1 [m]$, *chaque solution, après avoir subi une translation de vecteur* $\vec{v}(km, k'm)$, *reste une solution de l'équation.*

(*ii*)— Il se peut qu'en choisissant le carré, il y ait des solutions sur un bord du carré (donc sur l'autre aussi).

On considèrera deux solutions comme identiques si l'une peut être obtenue à partir de l'autre par translation.

De même, s'il y a 4 solutions dans les coins du carré, elles compteront pour une.

La recherche du nombre de solutions.

Nombre de solutions.

La « propriété du carré » va nous permettre de compter les solutions de l'équation : la connaissance des solutions dans un carré de côté p entraînant la connaissance de toutes les solutions, *on va définir le nombre de solutions à p près de l'équation comme le nombre de solutions de l'équation dans un carré de côté p.*

(voir remarque (*ii*) ci-avant)

Une conjecture.

En programmant notre calculatrice nous obtenons les résultats suivants :

p	nombre de solutions	p	nombre de solutions
2	*2 = p*	*61*	*60 = p–1*
3	**4 = *p* + 1**	**67**	**68 = *p* + 1**
5	*4 = p–1*	**71**	**72 = *p* + 1**
7	**8 = *p* + 1**	*73*	*72 = p–1*
11	**12 = *p* + 1**	**79**	**80 = *p* + 1**
13	*12 = p–1*	**83**	**84 = *p* + 1**
17	*16 = p–1*	*89*	*88 = p–1*
19	**20 = *p* + 1**	*97*	*96 = p–1*
23	**24 = *p* + 1**	*101*	*100 = p–1*
29	*28 = p–1*	**103**	**104 = *p* + 1**
31	**32 = *p* + 1**	**107**	**108 = *p* + 1**
37	*36 = p–1*	*109*	*108 = p–1*
41	*40 = p–1*	*113*	*112 = p–1*
43	**44 = *p* + 1**	**127**	**128 = *p* + 1**
47	**48 = *p* + 1**	**131**	**132 = *p* + 1**
53	*52 = p–1*	*137*	*136 = p–1*
59	**60 = *p* + 1**	**139**	**140 = *p* + 1**

A partir de ce tableau, de dimension limitée (il y a une infinité de nombres premiers), ***on conjecture*** l'expression du nombre de solutions de l'équation à p près, en fonction de p, de la façon suivante :

Conjecture 1 : (On distingue 3 cas.)

(i) Le cas qui semble unique **«** *2 = p* **»** : il y a 2 solutions.

(ii) Les cas **«** *p–1* **solutions »**, alors il semble que $p \equiv 1\ [4]$.

[en *italique* dans le tableau ci-dessus]

$$p \equiv 1\ [4] \Leftrightarrow (p-1) \in 4\mathbb{Z} \Leftrightarrow (p-1)/4 \in \mathbb{Z}$$

(iii) Les cas **« *p* + 1 solutions »**, alors il semble que $p \equiv 3\ [4]$.

[en **gras** dans le tableau ci-dessus]

$$p \equiv 3\ [4] \Leftrightarrow (p+1)/4 \in \mathbb{Z}$$

remarque :

2 est le seul nombre premier pair, les autres nombres premiers sont impairs, et donc

$$\text{soit } (p-1)/4 \in \mathbb{Z}, \text{ soit } (p+1)/4 \in \mathbb{Z}$$

ce qui signifie que notre conjecture porte sur TOUS les nombres premiers.

Transformation du problème.

Nous trouvant bloqués dans la démonstration de notre conjecture, Olivier Piltant nous propose de transformer le problème, et notamment d'essayer de factoriser l'expression.

Factorisation

Dans certaines conditions, on peut en effet, y arriver de la manière suivante :

On a $Kp \equiv 0\ [p]$, donc

$$x^2 + y^2 \equiv 1\ [p] \Leftrightarrow x^2 + y^2 + Kp \equiv 1\ [p]$$

(voir l'Annexe 1 : **Th. A** Transitivité).

On choisit K tel que $K = -ky^2$, $(k \in \mathbb{Z})$, donc

$$(1)\ x^2 + y^2 \equiv 1\ [p] \Leftrightarrow x^2 + y^2 - kpy^2 \equiv 1\ [p]$$

$$(1) \Leftrightarrow x^2 + (1-kp)y^2 \equiv 1\ [p]$$

$$(1) \Leftrightarrow x^2 - (kp-1)y^2 \equiv 1\ [p]$$

Pour pouvoir factoriser cette expression, de la forme $x^2 - Ay^2$, en gardant des coefficients entiers, il suffit que A soit un carré parfait (soit : $A = a^2$), c'est-à-dire que p puisse vérifier $kp - 1 = a^2$ avec $k \in \mathbb{Z}$, autrement dit que $-1 \equiv a^2\ [p]$.

(voir en Annexe 1 la **définition** de modulo)

Supposons que p vérifie $-1 \equiv a^2\ [p]$, donc :

$$x^2 + y^2 \equiv 1\ [p] \Leftrightarrow x^2 - a^2 y^2 \equiv 1\ [p]$$

$$x^2 + y^2 \equiv 1\ [p] \Leftrightarrow (x + ay)(x - ay) \equiv 1\ [p]$$

On pose : $X = x + ay$ et $Y = y - ay$.

On obtient :

$$x^2 + y^2 \equiv 1\ [p] \Leftrightarrow XY \equiv 1\ [p]$$

On étudie maintenant les solutions de

$$XY \equiv 1\ [p] \quad \text{équation } \mathbf{(2)}$$

(on vérifiera que $xy \equiv 1\ [p]$ et $XY \equiv 1\ [p]$ ont autant de solutions à p près, après cette étude qui est nécessaire).

Etude de $XY \equiv 1\ [p]$
… d'abord des préliminaires.

Pour cette étude, on travaille avec les classes de nombres (on note $\dot{n}$ est la « classe » de n.). La classe $\dot{n}$ représentera les nombres congrus à n modulo p, c'est-à-dire les nombres de la forme $n + kp$:

$$n,\ n+p,\ n+2p,\ \dots\ ,\ n-p,\ n-2p,\ \dots\ ,\ n+kp \quad (k \in \mathrm{Z}).$$

$\dot{0}$ représentera les nombres :

$$p,\ 2p,\ 3p,\ \dots\ ,\ -p,\ -2p,\ \dots\ ,\ kp \quad (k \in \mathrm{Z}).$$

On appelle alors Z/pZ l'ensemble de toutes ces classes :

$$\mathrm{Z}/p\mathrm{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dots, \dot{n}, \dots, \dot{p-1}\},$$

et on a :

$$\dot{p} = \dot{0},\ (\dot{n} + \dot{kp} = \dot{n}),\ \dots$$

Pour les opérations dans Z/pZ :

$$(\dot{a} + \dot{b}) = \dot{a} + \dot{b}$$
$$(\dot{a} \times \dot{b}) = \dot{a} \times \dot{b}$$

Etude de $XY \equiv 1\ [p]$ … nous y voilà.

On étudie l'équation en utilisant des tables de multiplication, le produit à un multiple de p près étant le reste de la division euclidienne de xy par p.

Les solutions de l'équation

$$XY \equiv 1\ [p]\ (\dot{X}\ \dot{Y} = \dot{1})$$

sont donc représentées par le $\dot{\mathbf{1}}$ dans le tableau. Par exemple :

Pour p = 3 :

×	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{\mathbf{1}}$	$\dot{2}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{\mathbf{1}}$

solutions :
$(\dot{1}, \dot{1})$ et $(\dot{2}, \dot{2})$

Pour p = 5 :

×	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{\mathbf{1}}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{\mathbf{1}}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{\mathbf{1}}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{\mathbf{1}}$

solutions : $(\dot{1}, \dot{1})$, $(\dot{2}, \dot{3})$, $(\dot{3}, \dot{2})$ et $(\dot{4}, \dot{4})$

Pour p = 7 :

×	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{\mathbf{1}}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{\mathbf{1}}$	$\dot{3}$	$\dot{5}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{2}$	$\dot{5}$	$\dot{\mathbf{1}}$	$\dot{4}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{\mathbf{1}}$	$\dot{5}$	$\dot{2}$	$\dot{6}$	$\dot{3}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{3}$	$\dot{\mathbf{1}}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{6}$	$\dot{0}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{\mathbf{1}}$

solutions :
$(\dot{1}, \dot{1})$, $(\dot{2}, \dot{4})$, $(\dot{3}, \dot{5})$, $(\dot{4}, \dot{2})$, $(\dot{5}, \dot{3})$ et $(\dot{6}, \dot{6})$.

Exemple de multiplication dans Z/pZ, **p n'étant pas premier : p = 6**

×	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{\mathbf{1}}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{\mathbf{1}}$

Conjecture 2 :

Lorsqu'on travaille dans Z/pZ (**p premier**) **pour chaque $\dot{X} \neq \dot{0}$, il existe un unique $\dot{Y}$ tel que $\dot{X}\ \dot{Y} = \dot{1}$ (ce qui n'est pas le cas si p n'est pas premier).**

Si cette conjecture était exacte, on aurait $p - 1$ solutions à p près pour l'équation $XY \equiv 1\ [p]$.

Démonstration de cette conjecture 2 :

On utilisera le **théorème (de Gauss)** :

Si p est premier, alors

$$ab \equiv 0\ [p] \Leftrightarrow a \equiv 0\ [p] \text{ ou } b \equiv 0\ [p].$$

Traduction dans $\mathbb{Z}/p\mathbb{Z}$:

$$\dot{X}\ \dot{Y} = \dot{0} \Leftrightarrow \dot{X} = \dot{0} \text{ ou } \dot{Y} = \dot{0}.$$

En effet, si on suppose que

$$ab \equiv 0\ [p],\ a \text{ Ú } 0\ [p] \text{ et } b \text{ Ú } 0\ [p],$$

p étant premier, on peut simplifier $ab \equiv 0\ [p]$, par a ou b (voir Annexe 1 : théorème C, corollaire 2). Alors $b \equiv 0\ [p]$ ou $a \equiv 0\ [p]$, ce qui est contraire aux hypothèses.

Pour démontrer la conjecture 2, on montre que pour un $\dot{X} \neq \dot{0}$, le nombre $\dot{X}\ \dot{Y}$ prend toutes les valeurs de $\mathbb{Z}/p\mathbb{Z}$, lorsqu'on fait varier $\dot{Y}$ dans $\mathbb{Z}/p\mathbb{Z}$. Considérons l'application (définie pour $\dot{X} \neq \dot{0}$) :

$$\begin{aligned} \varphi :\ & \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \\ & \dot{Y} \to \dot{X}\ \dot{Y} \end{aligned}$$

On veut montrer que φ est une bijection. En fait, pour montrer que φ est bijective, il suffit de montrer que φ est injective car :
• card $(\mathbb{Z}/p\mathbb{Z}) = p$, et est donc fini. (le nombre d'éléments de $\mathbb{Z}/p\mathbb{Z}$ est un nombre fini : p)
• et de plus, $\varphi :\ \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.
Donc, si chaque $\dot{Y}$ est l'unique antécédent de $\varphi(\dot{Y})$, les valeurs de $\varphi(\dot{0})$, $\varphi(\dot{1})$, $\varphi(\dot{2})$, …, $\varphi(\dot{p-1})$ seront différentes, et il ne "restera" pas de $\dot{z} \in \mathbb{Z}/p\mathbb{Z}$ n'ayant pas d'antécédent. Donc φ sera bijective.

Supposons qu'il existe plusieurs nombres $(\dot{Y}_1, \dot{Y}_2, \ldots, \dot{Y}_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ tels que

$$\varphi(\dot{Y}_1) = \varphi(\dot{Y}_2) = \ldots = \varphi(\dot{Y}_n)$$

On a alors :

$$\begin{aligned} \varphi(\dot{Y}_i) = \varphi(\dot{Y}_j) \quad & (i, j) \in \{1, 2, \ldots, n\}^2 \\ \varphi(\dot{Y}_i) = \varphi(\dot{Y}_j) &\Leftrightarrow \dot{X}\ \dot{Y}_i = \dot{X}\ \dot{Y}_j \\ \varphi(\dot{Y}_i) = \varphi(\dot{Y}_j) &\Leftrightarrow \dot{X}\ (\dot{Y}_i - \dot{Y}_j) = \dot{0} \\ \varphi(\dot{Y}_i) = \varphi(\dot{Y}_j) &\Leftrightarrow \dot{Y}_i - \dot{Y}_j = \dot{0} \text{ car } \dot{X} \neq \dot{0} \\ \varphi(\dot{Y}_i) = \varphi(\dot{Y}_j) &\Leftrightarrow \dot{Y}_i = \dot{Y}_j \end{aligned}$$

Donc φ réalise bien une injection (et donc une bijection, d'après ce qui précède) de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$.

Théorème 2 :

L'équation $XY \equiv 1\ [p]$ **a donc** $p - 1$ **solutions définies à** p **près ; à chaque** X **non congru à** 0 **modulo** p **, on peut associer un nombre et un seul, défini à** p **près, noté** X^{-1}**, tel que**

$$X\,X^{-1} \equiv 1\ [p]$$

X^{-1} **est alors l'inverse de** X**.**

Vérifions maintenant que
$x^2 + y^2 \equiv 1\ [p]$ et $XY \equiv 1\ [p]$
ont autant de solutions
quand p vérifie $-1 \equiv a^2\ [p]$.

On rappelle que :

$$x^2 + y^2 \equiv 1\ [p] \Leftrightarrow (x - ay)(x + ay) \equiv 1\ [p]$$

où $a = \sqrt{kp - 1}$, $a \in \mathbb{Z}$
et p vérifie $-1 \equiv a^2\ [p]$.

On veut réussir à faire entrer en bijection les ensembles de solutions des deux équations. On va faire correspondre à chaque solution de $XY \equiv 1[p]$ **(2)**, une solution de $x^2+y^2 \equiv 1[p]$ **(1)**. Puis on fera correspondre à chaque solution de **(1)** une solution de **(2)**.

On remarque que :

$$\begin{cases} X \equiv x - a\,y\ [p] \\ Y = x + a\,y\ [p] \end{cases} \Leftrightarrow \begin{cases} X + Y \equiv 2\,x\ [p] \\ Y - X = 2\,a\,y\ [p] \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 2^{-1}(X + Y)\ [p] \\ y \equiv (2\,a)^{-1}(Y - X)\ [p] \end{cases}$$

(2^{-1} et $(2a)^{-1}$ existent car $p \neq 2$.) On a donc deux applications :

$$\begin{cases} (i_1) : (X, Y) \to \left(2^{-1}(X + Y), (2\,a)^{-1}(Y - X)\right) \\ (i_2) : (x, y) \to (x - ay, x + ay) \end{cases}$$

On vérifie facilement que l'application (i_1) suivie de (i_2) redonne le couple (X, Y) à partir de (X, Y). De même (i_2) suivie de (i_1) associe (x, y) à (x, y). Les applications (i_1) et (i_2) sont donc des injections, réciproques l'une de l'autre. En conclusion, on a :

Théorème 3 :

L'équation $x^2 + y^2 \equiv 1\ [p]$ a $(p-1)$ solutions s'il existe un entier a tel que $-1 \equiv a^2\ [p]$.

Mais …

Quels sont les nombres p premiers pour lesquels il existe $a \in \mathbb{Z}$ tel que $-1 \equiv a^2\ [p]$?

Décompte des carrés parfaits.

Si l'on se place dans $\mathbb{Z}/p\mathbb{Z}$, on a tous les carrés parfaits sur la diagonale de la table de multiplication car ces carrés sont les produits d'un nombre par lui-même. (diagonale : n° de ligne = n° de colonne)

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	…	…	$\dot{p}-2$	$\dot{p}-1$
$\dot{0}$	$(\dot{0})^2$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$(\dot{1})^2$	$\dot{2}$	…	…		
$\dot{2}$	$\dot{0}$	$\dot{2}$	$(\dot{2})^2$				
…	$\dot{0}$	…		…			
…	$\dot{0}$	…			…		
$\dot{p}-2$	$\dot{0}$					$(\dot{p}-2)^2$	
$\dot{p}-1$	$\dot{0}$						$(\dot{p}-1)^2$

Il y a donc p carrés parfaits au maximum et $(p-1)$ si on enlève $\dot{0}$, qui est toujours présent. Mais, dans cette diagonale, il peut y avoir des nombres se répétant plusieurs fois.

Théorème 4 :

Si $p \neq 2$, chaque carré parfait (différent de $\dot{0}$) apparaît au moins deux fois sur la diagonale de la table de multiplication.

En effet, un nombre et son opposé ont le même carré : $(-\alpha)^2 = \alpha^2$. Dans le tableau, $-\dot{\alpha}$ est représenté par $\dot{p}-\dot{\alpha}$. Donc, chaque carré parfait (différent de $\dot{0}$) se répète au moins une fois.

Réciproquement, si un carré parfait apparaît, c'est deux fois : supposons que plusieurs nombres $\dot{a}_1, \dot{a}_2, \dot{a}_3, \ldots, \dot{a}_n$ aient le même carré, alors …

$$\dot{a}_1^2 = \dot{a}_2^2 = \dot{a}_3^2 = \ldots = \dot{a}_n^2.$$

Pour $(i, j) \in \{1, 2, \ldots, n\}^2$,

$$\begin{aligned} \dot{a}_i^2 = \dot{a}_j^2 &\Leftrightarrow \dot{a}_i^2 - \dot{a}_j^2 = \dot{0} \\ &\Leftrightarrow (\dot{a}_i - \dot{a}_j)(\dot{a}_i + \dot{a}_j) = \dot{0} \\ &\Leftrightarrow \dot{a}_i = \dot{a}_j \text{ ou } \dot{a}_i = -\dot{a}_j \end{aligned}$$

(d'après le théorème de Gauss ; cf. Annexe 1, théorème C, Corollaire 2)

… si un carré parfait apparaît, c'est deux fois.

On en déduit qu'il y a $(p-1)/2$ carrés parfaits ($\neq \dot{0}$), sauf si $p = 2$ car dans ce cas, il n'y a qu'un seul carré.

Théorème 5 :

Si un nombre $\dot{c}$ est un carré parfait, alors l'inverse de ce nombre est un carré parfait.

En effet, si $\dot{c} = \dot{b}^2$, alors $\dot{c}^{-1} = (\dot{b}^2)^{-1}$. Montrons que $(\dot{b}^2)^{-1} = (\dot{b}^{-1})^2$. On a :

$$\dot{b}\,\dot{b}^{-1} = \dot{1}$$

$$(\dot{b}\,\dot{b}^{-1})^2 = \dot{1}^2$$

$$\dot{b}^2\,(\dot{b}^{-1})^2 = \dot{1}$$

d'où :

$$\dot{b}^2 = ((\dot{b}^{-1})^2)^{-1}$$

$$(\dot{b}^2)^{-1} = (\dot{b}^{-1})^2 \quad (\text{car } (\dot{c}^{-1})^{-1} = \dot{c})$$

Donc, à chaque carré parfait, il correspond un autre carré parfait. Ce second carré parfait est différent du premier, sauf si le carré parfait de départ est $\dot{1}$ ou $-\dot{1}$; car ces deux nombres sont leur propre inverse, et ce sont les seuls avec cette propriété :

$$\begin{aligned} \dot{x} = \dot{x}^{-1} &\Leftrightarrow \dot{x}\,\dot{x} = \dot{x}\,\dot{x}^{-1} \\ &\Leftrightarrow \dot{x}^2 = \dot{1} \\ &\Leftrightarrow (\dot{x} - \dot{1})(\dot{x} + \dot{1}) = \dot{0} \\ &\Leftrightarrow \dot{x} = \dot{1} \text{ ou } \dot{x} = -\dot{1} \end{aligned}$$

Si on fait le décompte des carrés parfaits, on obtient :

- $\dot{1}$ *toujours présent car* $\dot{1}^2 = \dot{1}$
- *pour tout* $\dot{c}$ *carré parfait présent autre que* $\dot{1}$ *et* $-\dot{1}$, *il y a* $\dot{c}^{-1}$, *carré parfait*
- $-\dot{1}$ *quelquefois*

Résolution de la conjecture 1 dans le cas où il existe a tel que $-1 \equiv a^2\ [p]$.

Les $\frac{p-1}{2}$ carrés parfaits sont :

$$\dot{1}, \dot{-1}, \dot{c}_1, \dot{c}_1^{-1}, \dots, \dot{c}_n, \dot{c}_n^{-1}.$$

Il y en a donc un nombre pair, donc $\frac{p-1}{2}$ est divisible par 2. D'où

$$\frac{p-1}{4} \in \mathbb{Z}.$$

Donc $(p-1) \in 4\mathbb{Z}$ et $p \equiv 1\ [4]$.

Conclusion :

$-1 \equiv a^2\ [p] \Rightarrow p \equiv 1\ [4]$ (pour $p \neq 2$). (2 est un cas particulier car $\dot{-1} = \dot{1}$.)

Montrons **la réciproque** :

Soit p tel que $p \equiv 1\ [4]$.

Par hypothèse, $\frac{p-1}{4} \in \mathbb{Z}$, donc $\frac{p-1}{2}$ est divisible par 2.

Le nombre de carrés parfaits est donc pair. Or les carrés $\dot{1}, \dot{c}_1, \dot{c}_1^{-1}, \dots, \dot{c}_n, \dot{c}_n^{-1}$ sont présents, soit un nombre impair de carrés. Il manque donc un carré qui ne peut être que $\dot{-1}$ (le seul différent de $\dot{1}$ qui soit son propre inverse).

Donc : $p \equiv 1\ [4] \Rightarrow -1 \equiv a^2\ [p]$.

Théorème 6 :

Si p est un nombre premier autre que 2, alors $p \equiv 1\ [4] \Leftrightarrow$ il existe $a \in \mathbb{Z}$ tel que $-1 \equiv a^2\ [p]$.

On a vu que si p est tel que $-1 \equiv a^2\ [p]$, alors il y a $(p-1)$ solutions à p près de l'équation $x^2 + y^2 \equiv 1\ [p]$.

Corollaire :

L'équation $x^2 + y^2 \equiv 1\ [p]$ a $(p-1)$ solutions à p près quand $p \equiv 1\ [4]$.

Cela résout le cas (*ii*) de la conjecture 1.

Résolution de la conjecture 1 dans le cas $p \equiv 3\ [4]$.

Le cas $p \equiv 1\ [4]$ résolu, on se place dans le cas $p \equiv 3\ [4]$. $\dot{-1}$ n'est donc pas un carré parfait. On aimerait montrer qu'il y a alors $(p+1)$ solutions, ce qui n'est pas si éloigné des $(p-1)$ solutions de $XY \equiv 1\ [p]$.

On recherche donc un autre moyen de retrouver l'équation de l'hyperbole $XY \equiv 1\ [p]$, pour prouver que l'équation **(1)** a autant de solutions que l'équation de l'hyperbole $XY \equiv 1\ [p]$ plus deux autres solutions.

Plutôt que de rechercher directement à retrouver l'équation $XY \equiv 1\ [p]$, on va rechercher une équation de la forme $X^2 - Y^2 \equiv 1\ [p]$ qui a aussi $(p-1)$ solutions.

On veut donc passer de

$$x^2 + y^2 \equiv 1\ [p] \text{ à } X^2 - Y^2 \equiv 1\ [p].$$

Pour obtenir le signe "–", on écrit :

$$x^2 \equiv 1 - y^2\ [p]$$

On multiplie par l'inverse de x^2 :

$$1 \equiv (x^2)^{-1} - (x^2)^{-1} y^2\ [p]$$

Cependant, on a vu que seul $\dot{0}$ n'avait pas d'inverse, **on doit donc supposer que $x \neq \dot{0}$.**

(1) $x^2 + y^2 \equiv 1\,[p] \Leftrightarrow (x^2)^{-1} - (x^2)^{-1} y^2 \equiv 1[p]$
(1) $\Leftrightarrow (x^{-1})^2 - (x^{-1})^2 y^2 \equiv 1[p]$
(1) $\Leftrightarrow (x^{-1})^2 - (y\,x^{-1})^2 \equiv 1[p]$

On pose donc : $X \equiv x^{-1}\ [p]$ et $Y \equiv y\,x^{-1}\ [p]$. $X \equiv x^{-1}\ [p]$ donc on a aussi X Ú 0 $[p]$.

On a alors :

$$x \equiv X^{-1}\ [p]$$

et

$$y \equiv Y\,x \equiv Y\,X^{-1}\ [p]$$

On peut donc mettre en bijection …

• d'une part, l'ensemble des solutions de l'équation $x^2 + y^2 \equiv 1\ [p]$, hors des droites $x \equiv 0\ [p]$,

et …

• d'autre part, l'ensemble des solutions de $x^2 - y^2 \equiv 1\ [p]$, hors des droites $x \equiv 0[p]$.

On en déduit qu'il y a autant de solutions, hors des droites $x \equiv 0\ [p]$, pour les deux équations.

On compte les solutions sur les droites $x \equiv 0\ [p]$:

• équation $x^2 - y^2 \equiv 1[p]$:

$$x \equiv 0\ [p] \Rightarrow 0^2 - y^2 \equiv 1\ [p]$$
$$x \equiv 0\ [p] \Rightarrow y^2 \equiv -1\ [p]$$

ce qui n'a pas de solution quand $p \equiv 3\ [4]$. Il y a donc $p - 1$ solutions hors des droites $x \equiv 0\ [p]$ pour l'équation $x^2 - y^2 \equiv 1[p]$ donc aussi pour $x^2 + y^2 \equiv 1\ [p]$,

• équation $x^2 + y^2 \equiv 1\ [p]$, et sur $x \equiv 0\ [p]$:

$$x \equiv 0\ [p] \Rightarrow 0^2 + y^2 \equiv 1\ [p]$$
$$x \equiv 0\ [p] \Rightarrow (y + 1)(y - 1) \equiv 1\ [p]$$
$$x \equiv 0\ [p] \Rightarrow y \equiv 1[p] \text{ ou } y \equiv -1\ [p]$$

Il y a deux solutions sur $x \equiv 0\ [p]$.

Théorème 7:

L'équation $x^2 + y^2 \equiv 1[p]$ a $(p + 1)$ solutions à p près quand $p \equiv 3\ [4]$.

Conclusion.

Nous venons de résoudre le problème du nombre de solutions de $x^2 + y^2 \equiv 1\ [p]$, avec $(x, y, p) \in \mathbb{Z}^2 \times \mathbb{P}$ [NDLC : P désigne l'ensemble des nombres entiers naturels premiers.] ; nous nous sommes limités à un nombre p premier (permettant le rapprochement avec une hyperbole). Nous avons ainsi déterminé le nombre de solutions de l'équation $x^2 + y^2 \equiv 1\ [n]$, lorsque n est un nombre premier. Il resterait à voir ce qui se passe lorsque n est un entier quelconque, en commençant par le cas où n est une puissance d'un nombre premier, par exemple.

[NDLC : et pour un cercle « normal » (pas modulo p, mais pas forcément de rayon 1 non plus), combien y a-t-il de points à coordonnées entières ?]

Bibliographie :

Marc GUINOT, *Arithmétique pour amateurs*, tomes I et II, © 1992 Aléas éditeur.

[NDLC : on trouvera l'Annexe 1, annoncée précédemment, en page suivante ; elle est suivie d'une paramétrisation des solutions de $x^2 + y^2 \equiv 1\ [p]$: les solutions de l'équation s'obtiennent en donnant au paramètre chacune des valeurs possibles.]

ANNEXE 1 — Quelques théorèmes sur le langage des congruences dans Z.

Cette annexe va servir à énoncer des thèorèmes qui nous permettent de manipuler les congruences.

Définition 1
Soit $(a, b, c) \in \mathbb{Z}^3$, on dit que a est **congru à** b **modulo** p (noté $a \equiv b\ [p]$ ou $a \equiv b$ **modulo** p), si et seulement si $(a - b)$ est multiple de p, autrement dit $(a - b)/p \in \mathbb{Z}$, ou $(a - b) \in p\mathbb{Z}$, ou a est de la forme $b + kp$ $(k \in \mathbb{Z})$.

exemples :

$$3 \equiv 10\ [7] \text{ car } 3 = 10 - 1 \times 7$$
$$31 \equiv 13\ [3] \text{ car } 31 = 6 \times 3 + 13$$

Remarque : On dit alors que p est le **module** de la congruence.

Théorème A
Si $(a, b, c, p) \in \mathbb{Z}^4$, alors :
(*i*) : $a \equiv a\ [p]$ (réfléxivité)
(*ii*) : Si $a \equiv b\ [p]$ alors $b \equiv a\ [p]$ (symétrie)
(*iii*) : Si $a \equiv b\ [p]$ et $b \equiv c\ [p]$, alors $a \equiv c\ [p]$ (transitivité)

Définition 2
Si $p \in \mathbb{Z}$, on appelle classe de congruence modulo p de $a \in \mathbb{Z}$, l'ensemble des entiers congrus à a modulo p (c'est-à-dire l'ensemble des entiers de la forme $a + kp$).

Théorème B
Si $(a, p) \in \mathbb{Z} \times \mathbb{N}^*$, alors le reste dans la division euclidienne de a par p, est l'unique entier compris entre 0 et p - 1, congru à a modulo p :

$$a = qp + r \text{ avec } 0 \leq r \leq p - 1.$$

Corollaire
Si $(a, b, p) \in \mathbb{Z}^2 \times \mathbb{N}^*$, alors :

$a \equiv b\ [p] \Leftrightarrow a$ et b ont le même reste (r) dans la division euclidienne par p.

Théorème C
Si $(a, b, x, p) \in \mathbb{Z}^4$, alors :

$$(i)\ a \equiv b\ [p] \Leftrightarrow a + x \equiv b + x\ [p]$$
$$(ii)\ a \equiv b\ [p] \Rightarrow ax \equiv bx\ [p]$$

NB : La réciproque est vraie si x est premier avec p (c'est-à-dire s'ils n'ont que 1 ou -1 comme diviseurs communs).

Corollaire 1
Si $(a, b, c, p) \in \mathbb{Z}^4$, alors :

$$(i)\ a + b \equiv c\ [p] \Leftrightarrow a \equiv c - b\ [p]$$
$$(ii)\ a - b \equiv c\ [p] \Leftrightarrow a \equiv c + b\ [p]$$

Corollaire 2
Si $d|a$ (d divise a) et $d|b$ et si d est premier avec p, alors :

$$a \equiv b\ [p] \Leftrightarrow a/d \equiv b/d\ [p]$$

Théorème D
Soit $(a, b, p, x) \in \mathbb{Z}^3 \times \mathbb{Z}^*$, alors :

$$a \equiv b\ [p] \Leftrightarrow ax \equiv bx\ [px]$$

NB : Si $d|a$, $d|b$ et $d|p$, alors :

$$a \equiv b\ [p] \Leftrightarrow a/d \equiv b/d\ [p/d]$$

Théorème E
Si $a \equiv b\ [p]$ et $a' \equiv b'\ [p]$ alors

$$(i)\ a + a' \equiv b + b'\ [p]$$
$$(ii)\ a - a' \equiv b - b'\ [p]$$
$$(iii)\ aa' \equiv bb'\ [p]$$

[NDLC : P désigne l'ensemble des nombres entiers naturels premiers.]

Théorème F (dit **Petit théorème de Fermat)**
Si $(a, p) \in \mathbb{Z} \times \mathbb{P}$, alors $a^p \equiv a\ [p]$.
Et donc : si a Ú 0 $[p]$, alors $a^{p-1} \equiv 1\ [p]$
(cf. Th. 4, corollaire 2).

Théorème W (dit **Théorème de Wilson)**
$(p - 1)! \equiv -1\ [p] \Leftrightarrow p \in \mathbb{P}$

[NDLR : toutes les démonstrations de cette annexe sont laissées en exercice(s) au lecteur.]

ANNEXE 2 — Paramétrage des solutions.

Cette annexe va servir à exprimer les couples (x, y) solutions de l'équation en fonction d'un paramètre t et du nombre premier p.

Pour cela on utilise les formules de correspondance avec l'hyperbole.

[NDLR : On sépare l'étude en deux cas correspondant aux deux grandes classes de nombres p premiers : $p \equiv 1$ [4] et $p \equiv 3$ [4], laissant le cas $p = 2$ au lecteur.]

• si $p \equiv 1$ [4]

Si (X, Y) est solution de $XY \equiv 1$ [p], on a vu que les solutions de $x^2 + y^2 \equiv 1$ [p] s'obtiennent par :

$$x \equiv 2^{-1}\,(X + Y)\ [p]$$
$$y \equiv (2a)^{-1}\,(Y - X)\ [p]$$

où a est entier, vérifiant $a^2 \equiv -1$ [p].

Comme $XY \equiv 1$ [p], alors $Y \equiv X^{-1}$ [p], donc :

$$x \equiv 2^{-1}\,(X + X^{-1})\ [p]$$
$$y \equiv (2a)^{-1}\,(X^{-1} - X)\ [p]$$

De plus, d'après le *petit théorème de Fermat* [voir Annexe 1] :

$$\begin{array}{ll} & u^{p-1} \equiv 1\ [p] \\ \text{donc} & u.u^{p-2} \equiv 1\ [p] \\ \text{d'où} & u^{p-2} \equiv u^{-1}\ [p] \end{array}$$

Donc, avec $u = 2$ ou $u = 2a$ ou $u = X$:

$$x \equiv 2^{p-2}\,(X + X^{p-2})\ [p]$$
$$y \equiv (2a)^{p-2}\,(X^{p-2} - X)\ [p]$$

Cherchons à exprimer a tel que $a^2 \equiv -1$ [p], en fonction de p.

Pour cela on utilise le *théorème de Wilson* [voir Annexe 1] qui nous dit :

$$(p-1)! \equiv -1\ [p] \Leftrightarrow p \in \mathrm{P}.$$

On a $\dfrac{p-1}{4} \in \mathrm{Z}$, donc on peut dire :

$p-1 = 2m$ avec $m \in \mathrm{Z}$, m pair, et :

$$\begin{aligned}(p-1)! &= (2m)! \\ &= 1 \times 2 \times \ldots \times m \times (m+1) \\ &\qquad \times (m+2) \times \ldots \times (2m) \\ &= m!\,(p-1-m+1)\,(p-1-m+2) \\ &\qquad \ldots\,(p-1-m+m)\end{aligned}$$

car par hypothèse $2m = p-1 \Leftrightarrow m = p-1-m$.

$$(p-1)! = m!(p-m)(p-(m-1))(p-(m-2))\ldots(p-1)$$

Or $(p-\alpha)! \equiv -\alpha$ [p] et donc par transitivité :

$$\begin{aligned}(p-1)! &\equiv m!(p-m)(-1)(-2)\ldots(-m)\ [p] \\ &\equiv (-1)^m\, m\,!\, m\,!\ [p] \\ &\equiv (-1)^m\,(m\,!)^2\ [p]\end{aligned}$$

Or par hypothèse $\dfrac{p-1}{4} \in \mathrm{Z}$, donc $m = \dfrac{p-1}{2}$ est pair, donc $(-1)^m = 1$ et donc

$$(p-1)! \equiv (m\,!)^2\ [p]$$

et d'après le *théorème de Wilson* :

$$(p-1)! \equiv -1\ [p]$$

donc $(m\,!)^2 \equiv -1$ [p]. On en déduit qu'on peut prendre :

$$a \equiv m\,! \equiv \left(\frac{p-1}{2}\right)!\ [p]$$

On a donc, pour $x^2 + y^2 \equiv 1$ [p] et dans le cas où $p \equiv 1$ [4], un **paramétrage complet des solutions** en écrivant :

$$x \equiv 2^{p-2}\,(t + t^{p-2})\ [p]$$

$$y \equiv 2^{p-2}\left(\left(\frac{p-1}{2}\right)!\right)^{p-2}\,(t^{p-2} - t)\ [p]$$

$$t \in \{1, 2, 3, \ldots, p-1\}.$$

• **si $p \equiv 3$ [4]**

Dans ce cas, les formules de correspondance avec $XY \equiv 1$ [p] ne permettent pas de donner les solutions sur la droite $x = 0$. On doit donc ajouter deux solutions : $x \equiv 0$ [p], $y \equiv 1$ [p] et $x \equiv 0$ [p], $y \equiv -1$ [p]. On essaie d'exprimer les autres solutions en fonction de t, $t \in \{1, 2, 3, \dots, p-1\}$.

Les solutions de $X^2 - Y^2 \equiv 1$ [p] sont données par les formules :

$$X \equiv 2^{-1} (t + t^{-1}) \ [p]$$
$$Y \equiv 2^{-1} (t^{-1} - t) \ [p]$$
$$t \in \{1, 2, 3, \dots, p-1\}.$$

Pour retrouver $x^2 + y^2 \equiv 1$ [p] on doit poser $x \equiv X^{-1}$ [p] et $y \equiv Y\,x \equiv Y\,X^{-1}$ [p] :

$$x \equiv [2^{-1} (t + t^{-1})]^{-1} \ [p]$$
$$y \equiv 2^{-1} (t^{-1} - t)[2^{-1} (t + t^{-1})]^{-1} \ [p]$$

On a : $(\alpha\beta)^{-1} \equiv \alpha^{-1}\,\beta^{-1}$ car :

$(\alpha\beta)^{-1} \equiv (\alpha\beta)^{p-2} \equiv \alpha^{p-2}\,\beta^{p-2} \equiv \alpha^{-1}\,\beta^{-1} \dots$

$$x \equiv (2^{-1})^{-1} (t + t^{-1})^{-1} \ [p]$$
$$y \equiv 2^{-1} (t^{-1} - t)(2^{-1})^{-1} (t + t^{-1})^{-1} \ [p]$$

$$x \equiv 2 (t + t^{-1})^{-1} \ [p]$$
$$y \equiv 2^{-1}\,2 (t^{-1} - t) (t + t^{-1})^{-1} \ [p]$$

$$x \equiv 2 (t + t^{-1})^{-1} \ [p]$$
$$y \equiv (t^{-1} - t) (t + t^{-1})^{-1} \ [p]$$

$$x \equiv 2 (t + t^{p-2})^{p-2} \ [p]$$
$$y \equiv (t^{p-2} - t) (t + t^{p-2})^{p-2} \ [p]$$

Les solutions sont donc, quand $p \equiv 3$ [4] :

$$x \equiv 0 \ [p]$$
$$y \equiv 1 \ [p]$$

et
$$x \equiv 0 \ [p]$$
$$y \equiv -1 \ [p]$$

et
$$x \equiv 2 (t + t^{p-2})^{p-2} \ [p]$$
$$y \equiv (t^{p-2} - t) (t + t^{p-2})^{p-2} \ [p]$$
$$t \in \{1, 2, 3, \dots, p-1\}.$$