# Triplets pythagoriciens modulo un nombre premier

**Présentation**

Les calculs modulo un entier supérieur ou égal à 2 ont une illustration concrète.
En effet, selon le format que l'on choisit pour indiquer l'heure, on peut annoncer « il est treize heures. » ou « il est une heure. »

La correspondance entre « 13h » et « 1h » exprime que 13 est *congru* à 1 *modulo 12.*
De manière théorique, il est envisageable d'effectuer des calculs modulo n'importe quel nombre.

**Définition** Étant donnés deux entiers relatifs $a$ et $b$ et un entier naturel $n$ supérieur ou égal à 2, $a$ est congru à $b$ modulo $n$ signifie :

— $a$ a le même reste que $b$ dans la division euclidienne par $n$.
— La différence $a-b$ est un multiple de $n$.

Les deux propositions de cette définition sont équivalentes.

Il est immédiat que :

— si $a$ est congru à $b$ modulo $n$ alors $b$ est congru à $a$ modulo $n$.
— un nombre est congru à lui-même modulo $n$.
— étant donné $c$, nombre relatif, si $a$ est congru à $b$ modulo $n$, et si $b$ est congru à $c$ modulo $n$ alors $a$ est congru à $c$ modulo $n$

On aura reconnu une relation d'équivalence.

**Notation :**

$$a \equiv b \mod(n)$$

**Quelques propriétés**

$a, b, c, d$ sont des entiers relatifs, $k$ un entier naturel, $n$ un entier naturel supérieur ou égal à 2.

— $a \equiv b \mod(n)$ et $c \equiv d \mod(n) \Longrightarrow a+c \equiv b+d \mod(n)$
— $a \equiv b \mod(n)$ et $c \equiv d \mod(n) \Longrightarrow a \times c \equiv b \times d \mod(n)$
— $a \equiv b \mod(n) \Longrightarrow a^k \equiv b^k \mod(n)$

Il se trouve que c'est lorsque l'entier $n$ est un nombre premier que l'on a des propriétés intéressantes.
On rappelle qu'un nombre naturel $p$ est *premier* lorsqu'il possède exactement deux diviseurs, 1 et lui-même.
On considère alors l'ensemble des restes possibles dans la division euclidienne d'un nombre par $p$. Ce sont les classes d'équivalence de la relation d'équivalence. On note $\mathbf{Z}_p$ cet ensemble.

$$\mathbf{Z}_p = \{0, 1, \ldots, (p-1)\}$$

Et dans la suite, on considérera $\mathbf{Z}_p^* = \mathbf{Z}_p - \{0\}$.
L'avantage de $\mathbf{Z}_p^*$, lorsque $p$ est premier, est que c'est un groupe multiplicatif. En particulier, tout élément possède un inverse.
Exemple : $\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ comme $2 \times 4 \equiv 1 \mod(7)$
4 est l'inverse de 2 dans $\mathbf{Z}_7^*$

Un nombre premier $p$ étant donné, on se propose d'étudier l'équation

$$x^2 + y^2 \equiv z^2 \mod(p) \qquad (1)$$

où $x, y$ et $z$ sont dans $\mathbf{Z}_p^*$.
par exemple, pour $p = 17$, on a $2^2 + 3^2 \equiv 8^2 \mod(17)$ car :

$$2^2 + 3^2 \equiv 4 + 9 \equiv 13 \equiv 64 \mod(17)$$

Une solution $(a, b, c)$ de l'équation (1) est appelée *triplet pythagoricien modulo p*.

Il apparaît alors que si $(a, b, c)$ est une solution de (1) alors

$$\begin{array}{llll} (a,b,c) & (p-a,b,c) & (a,p-b,c) & (a,b,p-c) \\ (p-a,p-b,c) & (p-a,b,p-c) & (a,p-b,p-c) & (p-a,p-b,p-c) \end{array}$$

sont aussi solutions de (1). Il suffit de remarquer, par exemple, que $a$ et $p - a$ sont des nombres opposés modulo $p$. On dira que ces solutions sont *équivalentes*. L'objectif, ici, est de rechercher les solutions de (1) *non-équivalentes*.

Pour $p = 2$, on ne trouve qu'une solution : $1^2 + 1^2 = 0^2 \mod(2)$.
Cette solution n'est pas acceptable puisque $0 \notin \mathbf{Z}_p^*$.
On vérifie que pour $p = 3$ et $p = 5$, il n'y a aucune solution.
Pour $p = 7$, il y a trois solutions non-équivalentes :

$$2^2 + 5^2 = 1^2 \qquad 3^2 + 4^2 = 2^2 \qquad 1^2 + 6^2 = 3^2$$

Et pour $p = 11, 13, \ldots, 2017, \ldots$?

**Recherche de solutions**

**Un peu de théorie**

Pour tout élément $a \in \mathbf{Z}_p^*$, on note $\mathrm{ord}(a)$, le plus petit entier positif $n$ tel que $a^n = 1$. $\mathrm{ord}(a)$ est l'ordre de $a$.
$\langle a \rangle$ désigne le sous-groupe engendré par $a$. C'est-à-dire les puissances itérées de $a$.
Par exemple, avec $5 \in \mathbf{Z}_{11}^*$, on a $\langle 5 \rangle = \{5^1, 5^2, 5^3, 5^4, 5^5\} = \{5, 3, 4, 9, 1\}$ et $\mathrm{ord}(5) = 5$.

Le *Petit Théorème de Fermat* affirme que, pour un nombre premier $p$ et pour tout entier $a$ non divisible par $p$ on a :

$$a^{p-1} \equiv 1 \mod(p)$$

Ceci montre que $\langle a \rangle$ est cyclique.
Le *Théorème de Lagrange* indique que le nombre d'éléments d'un sous-groupe est un diviseur du nombre total d'éléments du groupe.

Ainsi, $\mathbf{Z}_{11}^*$ contenant 10 éléments, un sous-groupe de $\mathbf{Z}_{11}^*$ ne pourra contenir que 1, 2, 5 ou 10 éléments.
Si l'ordre d'un élément de $\mathbf{Z}_p^*$ est $p - 1$, c'est-à-dire le nombre d'éléments de $\mathbf{Z}_p^*$ alors on peut dire que $a$ est un générateur de $\mathbf{Z}_p^*$.
Un générateur de $\mathbf{Z}_p^*$ est appelé *racine primitive modulo p* et on démontre que pour tout nombre premier $p$, il existe des racines primitives modulo $p$.
On démontre également qu'étant donnés un nombre premier impair $p$ et un facteur $t$ de $p - 1$, le nombre d'éléments d'ordre $t$ de $\mathbf{Z}_p^*$ est $\varphi(t)$ qui est le nombre d'entiers entre 1 et $t$ qui sont premiers avec $t$.

**Exemple** : dans $\mathbf{Z}_{11}^*$

$$
\begin{array}{rll}
 & \text{sous-groupes} & \text{ord} \\
\langle 1\rangle = & \{1\} & 1 \\
\langle 2\rangle = & \{2,4,8,5,10,9,7,3,6,1\} & 10 \\
\langle 3\rangle = & \{3,9,5,4,1\} & 5 \\
\langle 4\rangle = & \{4,5,9,3,1\} & 5 \\
\langle 5\rangle = & \{5,3,4,9,1\} & 5 \\
\langle 6\rangle = & \{6,3,7,9,10,5,8,4,2,1\} & 10 \\
\langle 7\rangle = & \{7,5,2,3,10,4,6,9,8,1\} & 10 \\
\langle 8\rangle = & \{8,9,6,4,10,3,2,5,7,1\} & 10 \\
\langle 9\rangle = & \{9,4,3,5,1\} & 5 \\
\langle 10\rangle = & \{10,1\} & 2
\end{array}
$$

Remarques : $\varphi(5) = 4, \qquad \varphi(10) = 4$

Pour la suite , on aura besoin du lemme suivant :

**Lemme :**

Pour $x$ et $y$ dans $\mathbf{Z}_p^*$, si $\langle x\rangle \cap \langle y\rangle = \{1\}$ alors

$$\mathrm{ord}(xy) = \mathrm{PPCM}(\mathrm{ord}(x), \mathrm{ord}(y))$$

Preuve : soit $x, y \in \mathbf{Z}_p^*$. On note $n_1 = \mathrm{ord}(x)$, $n_2 = \mathrm{ord}(y)$ et $m = \mathrm{PPCM}(n_1, n_2)$. Soit $k_1$ et $k_2$ tels que : $m = k_1 \times n_1$ et $m = k_2 \times n_2$. Alors

$$(xy)^m = x^m y^m = x^{k_1 n_1} y^{k_2 n_2} = (x^{n_1})^{k_1} (y^{n_2})^{k_2} = (1)^{k_1}(1)^{k_2} = 1$$

Soit $s$, un entier naturel tel que $(xy)^s = 1$. La division de $s$ par $m$ donne un quotient $q$ et un reste $r$. On a alors

$$1 = (xy)^s = x^s y^s = x^{mq+r} y^{mq+r} = (x^m)^q x^r (y^m)^q y^r = x^r y^r$$

Puisque $\langle x\rangle \cap \langle y\rangle = \{1\}$ cela implique que $r = 0$ et $s$ est un multiple de $m$. D'où le résultat.

**Théorème :** Étant donné un nombre premier $p$ supérieur ou égal à 7, il existe des éléments $x$ et $y$ distincts de $\mathbf{Z}_p^*$ tels que

$$x^2 + y^2 \equiv 1 \mod(p)$$

Preuve : pour $p$ premier, $p \geqslant 7$, on considère $(a, b, c)$ un triplet particulier solution de (1) avec $a \neq b$. Par exemple, on peut vérifier que le triplet (3, 4, 5) est toujours solution. On envisage deux cas selon la parité de $\mathrm{ord}(c)$.

— 1er cas, si l'ordre de $c$ est pair. On écrit $\mathrm{ord}(c) = 2k + 2$ où $0 \leqslant k \leqslant (p-3)/2$. Alors

$$
\begin{array}{rll}
a^2 + b^2 & \equiv c^2 & \mod(p) \\
c^{2k}(a^2 + b^2) & \equiv c^{2k}(c^2) & \mod(p) \\
\left(c^k a\right)^2 + \left(c^k b\right)^2 & \equiv 1 & \mod(p)
\end{array}
$$

Remarque : $c^k a$ et $c^k b$ sont bien des éléments distincts de $\mathbf{Z}_p^*$.

— 2ième cas, si l'ordre de $c$ est impair. On remplace la solution particulière $(a, b, c)$ par la solution équivalente $(a, b, -c)$ ou $(a, b, p - c)$. Puis on applique le lemme avec $x = -1$ et $y = c$. Cela est possible car $\langle -1\rangle \cap \langle c\rangle = \{1\}$. En effet, nous avons $\langle -1\rangle = \{-1, 1\}$. Il faut donc s'assurer que $-1 \notin \langle c\rangle$ ce qui est le cas sinon l'ordre de $c$ serait pair.

Ce qui donne

$$\mathrm{ord}(-c) = \mathrm{ord}((-1) \times c) = \mathrm{PPCM}(\mathrm{ord}(-1), \mathrm{ord}(c)) = \mathrm{PPCM}(2, \mathrm{ord}(c))$$

Ainsi l'ordre de $(-c)$ est pair et on applique la méthode du premier cas.

**Corollaire :** Pour tout nombre premier $p$, supérieur ou égal à 7, chaque carré modulo $p$ peut s'écrire comme la somme de deux carrés distincts modulo $p$. En outre, l'équation (1) possède au moins $(p-1)/2$ solutions non équivalentes.

Preuve : Soit $p$ nombre premier, $p \geqslant 7$. D'après le théorème précédent, il existe $a, b \in \mathbf{Z}_p^*$ tels que

$$a^2 + b^2 \equiv 1 \mod(p)$$

Pour $c$ donné dans $\mathbf{Z}_p^*$, en multipliant les deux membres de l'équation par $c^2$, on obtient :

$$c^2(a^2 + b^2) \equiv c^2 \mod(p)$$

ou

$$(ca)^2 + (cb)^2 \equiv c^2 \mod(p)$$

Ainsi, l'équation (1) possède au moins une solution pour tout carré $c^2$ dans $\mathbf{Z}_p^*$. Comme il y a exactement $(p-1)/2$ carrés (résidus quadratiques) modulo $p$, le résultat en découle.

**Exemples**

Exemple avec $p = 11$

On part de la solution $(3, 4, 5)$ de (1) c'est-à-dire $3^2 + 4^2 \equiv 5^2 \mod(11)$
On a vu précédemment que $\mathrm{ord}(5) = 5$ dans $\mathbf{Z}_{11}^*$.
Comme $\mathrm{ord}(5)$ est impair,
on considère $\mathrm{ord}(-5) = \mathrm{ord}(6) = 10 = 2 \times 4 + 2$.
On obtient successivement :

$$\begin{array}{rll}
3^2 + 4^2 & \equiv 5^2 & \mod(11) \\
3^2 + 4^2 & \equiv 6^2 & \mod(11) \\
(6^4 \times 3)^2 + (6^4 \times 4)^2 & \equiv 6^{10} & \mod(11) \\
(6^4 \times 3)^2 + (6^4 \times 4)^2 & \equiv 1 & \mod(11) \\
(9 \times 3)^2 + (9 \times 4)^2 & \equiv 1^2 & \mod(11) \\
5^2 + 3^2 & \equiv 1^2 & \mod(11)
\end{array}$$

Puis, à partir de cette égalité, en multipliant les deux membres par les autres carrés de $\mathbf{Z}_{11}^*$, on obtient :

$$\begin{array}{lrll}
 & 5^2 + 3^2 & \equiv 1^2 & \mod(11) \\
\times 2^2 & (10)^2 + (6)^2 & \equiv 2^2 & \mod(11) \\
 & 1^2 + 5^2 & \equiv 2^2 & \mod(11) \\
\times 3^2 & (15)^2 + (9)^2 & \equiv 3^2 & \mod(11) \\
 & 4^2 + 2^2 & \equiv 3^2 & \mod(11) \\
\times 4^2 & (20)^2 + (12)^2 & \equiv 4^2 & \mod(11) \\
 & 2^2 + 1^2 & \equiv 4^2 & \mod(11) \\
\times 5^2 & (25)^2 + (15)^2 & \equiv 5^2 & \mod(11) \\
 & 3^2 + 4^2 & \equiv 5^2 & \mod(11)
\end{array}$$

**Combien de triplets-solutions modulo $p$**

Soit $N = N(p)$, le nombre total de solutions non-équivalentes de triplets pythagoriciens modulo $p$.
Pour $c \in \mathbf{Z}_p^*$ fixé, deux solutions non-équivalentes $(a_1, b_1, c)$ et $(a_2, b_2, c)$ sont appelées triplets *frères* pour $c$ modulo $p$ et on note $\sigma_p(c)$ le nombre de triplets frères pour $c$ modulo $p$.
S'il n'y a pas de frère pour $c$ modulo $p$, on posera $\sigma_p(c) = 1$. Ainsi,

$$N(p) = \sum_{c=1}^{(p-1)/2} \sigma_p(c)$$

Dans le cas $p = 19$, on obtient les solutions non-équivalentes :

$$\begin{array}{cccccc} (2,4,1) & (3,7,1) & (4,8,2) & (5,6,2) & (2,9,3) & (6,7,3) \\ (3,8,4) & (7,9,4) & (1,9,5) & (3,4,5) & (1,4,6) & (5,7,6) \\ (2,8,7) & (5,9,7) & (1,5,8) & (3,6,8) & (1,2,9) & (6,8,9) \end{array}$$

On observe que pour tout $c, 1 \leqslant c \leqslant 9$, il y a exactement 2 triplets frères modulo 19.
Et, le calcul de $N(19)$ donne :

$$N(19) = \sum_{c=1}^{(19-1)/2} \sigma_{19}(c) = \sum_{c=1}^{9} 2 = 9 \times 2 = 18$$

**Théorème** Pour tout nombre premier $p$ supérieur ou égal à 7
et pour tout $c, 1 \leqslant c \leqslant (p-1)/2$,
le nombre $\sigma_p(c)$ est constant.

Preuve : Il suffit de montrer que, pour tout $c, 1 \leqslant c \leqslant (p-1)/2$, $\sigma_p(c) = \sigma_p(1)$ où $p$, est un nombre premier supérieur ou égal à 7 .
Pour cela, on reprend l'idée utilisée dans la preuve du corollaire précédent. Si $(a_1, b_1, 1)$ et $(a_2, b_2, 1)$ sont des triplets frères pour 1 modulo $p$ alors, $(ca_1, cb_1, c)$ et $(ca_2, cb_2, c)$ sont triplets frères pour $c$ modulo $p$.
Réciproquement, si $(d_1, e_1, c)$ et $(d_2, e_2, c)$ sont triplets frères pour $c$ modulo $p$ alors $(c^{-1}d_1, c^{-1}e_1, 1)$ et $(c^{-1}d_2, c^{-1}e_2, 1)$ sont triplets frères pour 1 modulo $p$. Il en résulte qu'il y a bijection entre l'ensemble des triplets frères pour 1 modulo $p$ et l'ensemble des triplets frères pour $c$ modulo $p$. Ce qui établit le théorème.

On en déduit le résultat suivant :
**Corollaire :**
Pour tout nombre premier $p$ supérieur ou égal à 7,

$$N(p) = \frac{p-1}{2}\sigma_p(1)$$

**Définition :** Soit $p$ un nombre premier supérieur ou égal à 7 .
Un triplet pythagoricien $(a, b, c)$ modulo $p$ sera dit *isocèle* lorsque $a^2 \equiv b^2 \mod(p)$

On observe qu'il n'y a pas de triplet pythagoricien isocèle modulo 19. En revanche, avec $p = 17$, les triplets solutions sont :

$$\begin{array}{cccc} (3,3,1) & (4,6,1) & (5,8,2) & (6,6,2) \\ (1,5,3) & (8,8,3) & (1,7,4) & (5,5,4) \\ (2,2,5) & (3,4,5) & (1,1,6) & (2,7,6) \\ (4,4,7) & (6,8,7) & (2,3,8) & (7,7,8) \end{array}$$

On note que pour tout $c, 1 \leqslant c \leqslant 8$, il y a un triplet frère avec $a^2 \equiv b^2 \mod(17)$.
Comment expliquer l'absence ou la présence de triplets isocèles parmi les triplets pythagoriciens modulo $p$ ?

On va montrer que cela dépend si 2 est un carré modulo $p$ ou pas.
On remarque déjà que $6^2 \equiv 2 \mod(17)$ donc 2 est un carré modulo 17.
Tandis que les carrés de $\mathbf{Z}_{19}^*$ sont $\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2\} = \{1, 4, 9, 16, 6, 17, 11, 7, 5\}$.

**Théorème :** Étant donné un nombre premier $p$ supérieur ou égal à 7, il existe des triplets pythagoriciens isocèles modulo $p$ si et seulement si 2 est un carré modulo $p$.
En outre, si 2 est un carré modulo $p$, il y a exactement $(p-1)/2$ triplets pythagoriciens isocèles non-équivalents. Un pour chaque valeur de $c, 1 \leqslant c \leqslant (p-1)/2$.

Preuve : soit un nombre premier $p$ supérieur ou égal à 7.
Premièrement, si $(a, b, c)$ est un triplet pythagoricien isocèle modulo $p$ alors il en est de même pour $(c^{-1}a, c^{-1}b, 1)$.

Réciproquement, si $(a, b, 1)$ est un triplet pythagoricien isocèle modulo $p$ alors il en est de même pour $(ca, cb, c)$.
Ceci montre que s'il existe un triplet pythagoricien isocèle modulo $p$ alors il y en a au moins $(p-1)/2$, un pour chaque $c, 1 \leqslant c \leqslant (p-1)/2$.
Deuxièmement, si $(a, b, 1)$ et $(d, e, 1)$ sont deux triplets pythagoriciens isocèles modulo $p$ ceci implique que :
$a^2 \equiv b^2$ et $d^2 \equiv e^2 \mod(p)$ ainsi

$$\begin{array}{rlll} a^2 + a^2 & \equiv 1 & \equiv d^2 + d^2 & \mod(p) \\ 2a^2 & \equiv 2d^2 & & \mod(p) \\ a^2 & \equiv d^2 & & \mod(p) \end{array}$$

Ceci montre que les triplets $(a, b, 1)$ et $(d, e, 1)$ sont équivalents.
Il en résulte qu'il y a au plus $(p-1)/2$ triplets pythagoriciens isocèles modulo $p$.

Enfin, si 2 est un carré modulo $p$ cela signifie qu'il existe $t \in \mathbf{Z}_p^*$ tel que $t^2 = 2$ alors il est immédiat que $(1, 1, t)$ est un triplet pythagoricien isocèle modulo $p$.
Réciproquement, si $(1, 1, t)$ est un triplet pythagoricien isocèle modulo $p$ alors, $t^2 = 2$ ce qui montre que 2 est un carré modulo $p$.

On démontre que 2 est un carré modulo $p$ ( $p$, nombre premier impair) si et seulement si $p \equiv 1$ ou $-1 \mod(8)$.
On en déduit le corollaire suivant :
**Corollaire :** Étant donné un nombre premier $p \geqslant 7$, il existe des triplets pythagoriciens isocèles modulo $p$ si et seulement si

$$p \equiv \pm 1 \mod(8)$$

C'est ce qui a été observé avec $p = 17$, $17 \equiv 1 \mod(8)$
Tandis qu'avec $p = 19$, $19 \equiv 3 \mod(8)$ donc pas de triplets isocèles.

Pour conclure, un théorème admis :
**Théorème :** Pour tout nombre premier $p \geqslant 7$

$$\sigma_p(1) = \begin{cases} \dfrac{p-1}{8} & \text{si } p \equiv 1 \mod(8) \\ \dfrac{p-3}{8} & \text{si } p \equiv 3 \mod(8) \\ \dfrac{p-5}{8} & \text{si } p \equiv 5 \mod(8) \\ \dfrac{p+1}{8} & \text{si } p \equiv 7 \mod(8) \end{cases}$$

Rappel : $\sigma_p(1)$ désigne le nombre de triplets frères pour 1 modulo $p$.

Exemple : pour $p = 23$, on a $23 \equiv -1 \mod(8)$, $\dfrac{p+1}{8} = 3$ soit $\sigma_{23}(1) = 3$

$$\begin{aligned}
4^2 + 10^2 &\equiv 1^2 \qquad \mod(23)\\
8^2 + 11^2 &\equiv 1^2 \qquad \mod(23)\\
9^2 + 9^2 &\equiv 1^2 \qquad \mod(23)
\end{aligned}$$

### Algorithmique

**Entrées :** $p$, nombre premier supérieur ou égal à 7
**Initialisation :**
compteur $\leftarrow 0$
**Traitement :**
**pour** $a$ **allant de** 1 **à** $(p-1)/2$ **faire**
  $aa \leftarrow a^2 \quad \mathrm{mod}(p)$
  **pour** $b$ **allant de** 1 **à** $(p-1)/2$ **faire**
    $bb \leftarrow b^2 \quad \mathrm{mod}(p)$
    **pour** $c$ **allant de** 1 **à** $(p-1)/2$ **faire**
      $cc \leftarrow c^2 \quad \mathrm{mod}(p)$
      **si** $(aa+bb) \quad mod(p) == cc$ **et** $a <= b$ **alors**
        afficher : $a^2+b^2=c^2 \quad \mathrm{mod}(p)$
        compteur$\leftarrow$ compteur + 1
**Afficher :** compteur

**Algorithme 1 :** Force brute

### Avec Ruby

Suggestion de programme en Ruby :

```ruby
puts " valeur de p, nombre premier supérieur ou égal à 7?"
p = gets.to_i
compteur = 0
debut = Time.now
for a in 1..(p-1)/2
    aa = (a ** 2) % p
    for b in 1..(p-1)/2
        bb = (b ** 2) % p
        for c in 1..(p-1)/2
          cc = (c ** 2) % p
          if (aa + bb) % p == cc  and a <= b
              puts " #{a}^2 + #{b}^2 = #{c}^2  (mod#{p})"
              compteur = compteur + 1
          end
        end
    end
end
puts " Pour p = #{p}, il y a  #{compteur} solutions non-équivalentes."
fin = Time.now
puts " temps #{fin - debut} secondes pour force brute"
```

Et sa réponse :

```
21^2 + 28^2 = 24^2  (mod59)
22^2 + 24^2 = 23^2  (mod59)
22^2 + 28^2 = 18^2  (mod59)
22^2 + 29^2 = 26^2  (mod59)
23^2 + 26^2 = 5^2  (mod59)
23^2 + 27^2 = 14^2  (mod59)
23^2 + 28^2 = 29^2  (mod59)
24^2 + 25^2 = 27^2  (mod59)
24^2 + 27^2 = 19^2  (mod59)
24^2 + 28^2 = 11^2  (mod59)
24^2 + 29^2 = 1^2  (mod59)
25^2 + 26^2 = 11^2  (mod59)
26^2 + 27^2 = 15^2  (mod59)
27^2 + 29^2 = 6^2  (mod59)
Pour p = 59, il y a  203 solutions non-équivalentes.
temps 0.01601 secondes pour force brute
```

### Avec Python 3

Suggestion de programme en Python 3 :

```
from time import clock
p = eval(input("valeur de p, nombre premier supérieur ou égal à 7 ?"))
debut = clock()
compteur = 0
for a in range(1, int((p - 1) / 2 + 1)):
    aa = a ** 2 % p
    for b in range(1, int((p - 1) / 2 + 1)):
        bb = b ** 2 % p
        for c in range(1, int((p - 1) / 2 + 1)):
            cc = c ** 2 % p
            if (aa + bb) % p == cc and a <= b:
                print(str(a)+'^2 + '+str(b)+'^2 = '+str(c)+'^2     mod('+str(p)+')')
                compteur = compteur + 1
print(' Pour p = '+str(p)+', il y a '+str(compteur)+' solutions non équivalentes')
fin = clock()
duree = fin - debut
print(' temps de calcul : '+str(duree)+' s pour force brute')
```

Réponse :

```
23^2 + 28^2 = 29^2     mod(59)
24^2 + 25^2 = 27^2     mod(59)
24^2 + 27^2 = 19^2     mod(59)
24^2 + 28^2 = 11^2     mod(59)
24^2 + 29^2 = 1^2     mod(59)
25^2 + 26^2 = 11^2     mod(59)
26^2 + 27^2 = 15^2     mod(59)
27^2 + 29^2 = 6^2     mod(59)
 Pour p = 59, il y a 203 solutions non équivalentes
 temps de calcul : 0.253831 s pour force brute
```

### Avec scilab

Suggestion de programme en scilab :

```
p = input("Valeur de p, nombre premier supérieur ou égal à 7 ?" );
tic();
compteur = 0;
for a=1:(p-1)/2
    aa=reste(a^2,p);
    for b=1:(p-1)/2
        bb=reste(b^2, p);
        for c=1:(p-1)/2
            cc=reste(c^2,p);
            if reste(aa+bb,p)==cc & a<=b  then
                disp(''+string(a)+'^2 + '+string(b)+'^2 = '+string(c)+'^2    mod('+string(p)+')');
                compteur = compteur + 1;
            end
         end
     end
end
disp(' pour p = '+string(p)+ ', il y a '+string(compteur)+' solutions non équivalentes.')
t = toc();
disp('temps = '+string(t)+' avec force brute');
```

Réponse :

```
23^2 + 28^2 = 29^2     mod(59)

24^2 + 25^2 = 27^2     mod(59)

24^2 + 27^2 = 19^2     mod(59)

24^2 + 28^2 = 11^2     mod(59)

24^2 + 29^2 = 1^2     mod(59)

25^2 + 26^2 = 11^2     mod(59)

26^2 + 27^2 = 15^2     mod(59)

27^2 + 29^2 = 6^2     mod(59)

 pour p = 59, il y a 203 solutions non équivalentes.

temps = 1.854 avec force brute
```

### Variantes

D'après ce qui précède, on peut essayer de rendre le calcul plus efficace :

**Entrées :** $p$, nombre premier supérieur ou égal à 7
**Initialisation :**
compteur $\leftarrow 0$
$c \leftarrow 1$
**Traitement :**
**pour** $a$ **allant de** 1 **à** $(p-1)/2$ **faire**
  $aa \leftarrow a^2 \mod(p)$
  **pour** $b$ **allant de** 1 **à** $(p-1)/2$ **faire**
    $bb \leftarrow b^2 \mod(p)$
    **si** $(aa+bb) \quad mod(p) == c$ **et** $a <= b$ **alors**
      $s1 \leftarrow [a, b, c]$
      **pour** $k$ **allant de** 1 **à** $(p-1)/2$ **faire**
        $sk[0] \leftarrow \min(k \times a \mod(p), p - k \times a \mod(p))$
        $sk[1] \leftarrow \min(k \times b \mod(p), p - k \times b \mod(p))$
        $sk[2] \leftarrow \min(k \times c \mod(p), p - k \times c \mod(p))$
        $sk \leftarrow [sk[0], sk[1], sk[2]]$
        **si** $sk[0] > sk[1]$ **alors**
          échanger $sk[0]$ et $sk[1]$
          afficher $sk$
          compteur $\leftarrow$ compteur + 1
**Afficher** : compteur

**Algorithme 2 :** Subtil.

Suggestion de programme en Ruby :

```ruby
puts " valeur de p, nombre premier supérieur ou égal à 7?"
p = gets.to_i
compteur = 0
c = 1
debut = Time.now
for a in 1..(p-1)/2
    aa = (a ** 2) % p
    for b in 1..(p-1)/2
        bb = (b ** 2) % p
        if (aa + bb) % p == c  and a <= b
             s = [a, b, c] # a^2 + b^2 = 1^2
            for k in 1..(p-1)/2 # à partir de cette solution, on déduit les autres
            #par multiplication membre à membre par k
                sk = s.collect{|obj| [(k * obj) % p, p - ((k * obj) % p)].min} # pour
                #ne garder que les valeurs les plus petites
                if sk[0] > sk[1] # sinon on obtient une solution équivalente.
                #On souhaite présenter les solutions a^2 + b^2 = c^2  avec a <= b
                    temp = sk[0]
                    sk[0] = sk[1]
                    sk[1] = temp
                end
                puts " #{sk[0]}^2 + #{sk[1]}^2 = #{sk[2]}^2  (mod#{p})"
                compteur = compteur + 1
            end
        end
    end
end
puts " Pour p = #{p}, il y a  #{compteur} solutions non-équivalentes."
fin = Time.now
puts " temps #{fin - debut} secondes pour subtil"
```

Réponse :

```
8^2 + 29^2 = 16^2  (mod59)
5^2 + 21^2 = 17^2  (mod59)
9^2 + 19^2 = 18^2  (mod59)
16^2 + 20^2 = 19^2  (mod59)
8^2 + 10^2 = 20^2  (mod59)
19^2 + 27^2 = 21^2  (mod59)
3^2 + 11^2 = 22^2  (mod59)
18^2 + 21^2 = 23^2  (mod59)
12^2 + 14^2 = 24^2  (mod59)
10^2 + 17^2 = 25^2  (mod59)
13^2 + 25^2 = 26^2  (mod59)
1^2 + 16^2 = 27^2  (mod59)
14^2 + 23^2 = 28^2  (mod59)
12^2 + 15^2 = 29^2  (mod59)
Pour p = 59, il y a  203 solutions non-équivalentes.
temps 0.006542 secondes pour subtil
```

Suggestion de programme en Python 3 :

```python
from time import clock
p = eval(input("valeur de p, nombre premier supérieur ou égal à 7 ?"))
debut = clock()
compteur = 0
c = 1
for a in range(1, int((p - 1) / 2 + 1)):
    aa = a ** 2 % p
    for b in range(1, int((p - 1) / 2 + 1)):
        bb = b ** 2 % p
        if (aa + bb) % p == c and a <= b:
            s1 = [a, b, c]
            for k in range(1, int((p - 1) / 2 + 1)):
                ss = [min((k * x) % p, p - ((k * x) % p)) for x in s1]
                if ss[0] > ss[1]:
                    [ss[0], ss[1]] = [ss[1], ss[0]]
                compteur = compteur + 1
                print(str(ss[0])+'^2 + '+str(ss[1])+'^2 = '+str(ss[2])+'^2    mod('+str(p)+')')
print(' Pour p = '+str(p)+', il y a '+str(compteur)+' solutions non équivalentes')
fin = clock()
duree = fin - debut
print(' temps de calcul : '+str(duree)+'s pour subtil')
```

Réponse :

```
8^2 + 10^2 = 20^2    mod(59)
19^2 + 27^2 = 21^2    mod(59)
3^2 + 11^2 = 22^2    mod(59)
18^2 + 21^2 = 23^2    mod(59)
12^2 + 14^2 = 24^2    mod(59)
10^2 + 17^2 = 25^2    mod(59)
13^2 + 25^2 = 26^2    mod(59)
1^2 + 16^2 = 27^2    mod(59)
14^2 + 23^2 = 28^2    mod(59)
12^2 + 15^2 = 29^2    mod(59)
 Pour p = 59, il y a 203 solutions non équivalentes
 temps de calcul : 0.22031699999999999s pour subtil
```

Suggestion de programme en scilab :

```
p = input("Valeur de p, nombre premier supérieur ou égal à 7 ?" );
tic();
compteur = 0;
for a=1:(p-1)/2
    aa=reste(a^2,p);
    for b=1:(p-1)/2
        bb=reste(b^2, p);
        if reste(aa+bb,p)==1 & a<=b  then
            c = 1;
            s1 = [a, b, c];
            for k = 1:(p-1)/2
                sk = k * s1;
                for j = 1:3
                    sk(j)=min(reste(sk(j), p), p-reste(sk(j), p));
                end
                disp(''+string(sk(1))+'^2 + '+string(sk(2))+'^2 = '+string(sk(3))+'^2    mod('+string(p)+')');
                compteur = compteur +1;
            end
        end
    end
end
disp(' pour p = '+string(p)+ ', il y a '+string(compteur)+' solutions non équivalentes.')
t = toc();
disp('temps = '+string(t)+' avec subtil');
```

Réponse :

```
14^2 + 12^2 = 24^2    mod(59)

10^2 + 17^2 = 25^2    mod(59)

25^2 + 13^2 = 26^2    mod(59)

1^2 + 16^2 = 27^2    mod(59)

23^2 + 14^2 = 28^2    mod(59)

12^2 + 15^2 = 29^2    mod(59)

 pour p = 59, il y a 203 solutions non équivalentes.

temps = 0.312 avec subtil
```

**Bibliographie**


— B. M. MOORE - H. J. STRAIGHT, *Pythagorean Triples Modulo a Prime*, ΠME Journal, Vol 13, No 10, pp 651-659.

— Rémi GOBLOT, *Algèbre commutative*, Masson ISBN 2-225-85308-8

— Math Term S, Collection Hyperbole, Programme 2002, Editions Nathan ISBN 209-172460-2

— http://www.math.brown.edu/~jhs/Frint4thChapter21.pdf

**Annexe**

## Petit théorème de Fermat

**Petit théorème de Fermat** $p$ est un nombre premier, $a$ est un entier supérieur ou égal à 2 et non divisible par $p$. Alors
$$a^{p-1} \equiv 1 \mod(p)$$

Preuve :

- $p$ est un nombre premier alors $p$ est premier avec tous les entiers non nuls qui lui sont strictement inférieurs, $1, 2, \ldots, p-1$. Ainsi $p$ est premier avec leur produit, c'est-à-dire, $(p-1)!$.
- Si $k$ est un entier tel que $1 \leqslant k \leqslant p-1$ alors le reste de la division euclidienne de $ka$ par $p$, noté $r_k$, est non nul. En effet, si $p$ divise $ka$, comme $p$ est premier avec $k$, d'après le théorème de Gauss, $p$ devrait diviser $a$ ce qui n'est pas par hypothèse.
- Si $k'$ est un entier distinct de $k$ tel que $1 \leqslant k' \leqslant p-1$, alors les restes $r_k$ et $r'_k$ des divisions respectives de $ka$ et $k'a$ par $p$ sont distincts. Sinon, si $r_k = r'_k$ supposons par exemple que $k > k'$ alors $(k-k')a$ serait divisible par $p$ or $p$ est premier avec $k-k'$ et ne divise pas $a$ donc c'est impossible.
- Ainsi les $p-1$ divisions par $p$ ont des restes distincts, non nuls. Ce sont donc, à l'ordre près, les entiers $1, 2, \ldots, p-1$
- En multipliant membre à membre les $p-1$ congruences $ka \equiv r_k \mod(p)$ nous obtenons $(p-1)!a^{p-1} \equiv (p-1)! \mod(p)$. $p$ étant premier avec $(p-1)!$ nous en déduisons $a^{p-1} \equiv 1 \mod(p)$.

**Théorème de Lagrange**

Soit $(G, \cdot)$ un groupe d'ordre fini dont la loi est notée multiplicativement. Soit $H$ un sous-groupe de $(G, \cdot)$. Alors, l'ordre de $H$ divise l'ordre de $G$.

Pour la preuve de ce théorème, nous utiliserons la proposition suivante :
**Proposition** Soit $(G, \cdot)$ un groupe et $H$ un sous-groupe de $G$. La relation définie sur $G$ par

$$\forall x \in G, \forall y \in G, \quad x\mathscr{R}y \text{ si et seulement si } x^{-1} \cdot y \in H$$

est une relation d'équivalence et, pour tout $x \in G$, la classe d'équivalence de $x$, $cl(x)$ est de la forme :

$$cl(x) = x \cdot H = \{x \cdot y | y \in H\}$$

Preuve :

- Pour tout $x \in G$, nous avons $x^{-1} \cdot x = e$. $H$ étant un sous-groupe, $e \in H$ ce qui entraine $x\mathscr{R}x$ et prouve que $\mathscr{R}$ est *réflexive*.
- Pour tout $x \in G$, et tout $y \in G$ tels que $x\mathscr{R}y$, c'est-à-dire $x^{-1} \cdot y \in H$, le symétrique de $x^{-1} \cdot y$ est un élément de $H$ puisque $H$ est un groupe. Or, $\left(x^{-1} \cdot y\right)^{-1} = y^{-1} \cdot x$ ce qui exprime que $y\mathscr{R}x$ et prouve que $\mathscr{R}$ est *symétrique*.
- Soit $x, y, z$ éléments de $G$ tels que $x\mathscr{R}y$ et $y\mathscr{R}z$. Nous avons

  $$x^{-1} \cdot z = x^{-1} \cdot e \cdot z = x^{-1} \cdot y \cdot y^{-1} \cdot z = (x^{-1} \cdot y) \cdot (y^{-1} \cdot z)$$

  Puisque $H$ est un groupe, $(x^{-1} \cdot y) \cdot (y^{-1} \cdot z) \in H$ c'est-à-dire $x^{-1} \cdot z \in H$ ce qui prouve que $\mathscr{R}$ est *transitive*.

$\mathscr{R}$ est donc une relation d'équivalence.

Voyons maintenant les *classes d'équivalence* de cette relation. Pour $x \in G$, $cl(x)$ est définie par

$$cl(x) = \{y \in G | x\mathscr{R}y\} = \{y \in G | x^{-1} \cdot y \in H\}$$

— Soit $y \in cl(x)$. Nous pouvons écrire $y = x \cdot x^{-1} \cdot y = x \cdot (x^{-1} \cdot y)$. Comme $x^{-1} \cdot y \in H$, $y$ est de la forme $x \cdot z$ où $z \in H$. Nous en déduisons que $cl(x) \subset x \cdot H$.

— Soit $y \in x \cdot H$. Cela signifie qu'il existe $z \in H$ tel que $y = x \cdot z$. Nous avons $x^{-1} \cdot y = x^{-1} \cdot x \cdot z = z$ ce qui montre que $x^{-1} \cdot y \in H$ et donc $x \mathscr{R} y$ c'est-à-dire $y \in cl(x)$ ce qui établit que $x \cdot H \subset cl(x)$.

En conclusion $x \cdot H = cl(x)$.

Nous pouvons désormais revenir à la preuve du théorème de Lagrange.
Notons $n = Card(G)$ et $p = Card(H)$.
Pour tout $x \in H$, l'ensemble $cl(x) = x \cdot H$ contient le même nombre d'éléments que $H$.
En effet, soit $y_1$ et $y_2$ éléments de $H$, nous avons $x \cdot y_1 = x \cdot y_2 \Longrightarrow y_1 = y_2$ puisque dans un groupe, tout élément est régulier. Par contraposition, nous avons, si $y_1 \neq y_2 \Longrightarrow x \cdot y_1 \neq x \cdot y_2$. Les ensembles $H$ et $x \cdot H$ ont donc le même cardinal.
L'ensemble des classes d'équivalence forme une partition de $G$.
Soit $r$ le nombre (fini) de ces classes d'équivalence distinctes, chaque classe contient $p$ éléments, nous avons donc $p \times r = n$.

**Critère d'Euler**

$p$ est un nombre premier impair.
$a \in \mathbf{Z}_p^*$, est un carré si et seulement si $a^{\frac{p-1}{2}} \equiv 1 \mod(p)$

Preuve :

— Si $a$ est un carré de $\mathbf{Z}_p^*$ alors il existe $b \in \mathbf{Z}_p^*$ tel que $a = b^2$ et donc $a^{\frac{p-1}{2}} = b^{2 \cdot \frac{p-1}{2}} = b^{p-1} = 1$ d'après le petit théorème de Fermat. Ainsi $a$ est une solution de $X^{\frac{p-1}{2}} - 1 \equiv 0 \mod(p)$

— Ce polynôme de degré $\frac{p-1}{2}$ n'a pas d'autres racines que les $\frac{p-1}{2}$ carrés de $\mathbf{Z}_p^*$. Si $a$ n'est pas un carré de $\mathbf{Z}_p^*$, le petit théorème de Fermat donne :

$$0 \equiv a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \mod(p)$$

Nous venons de voir que le premier facteur est non nul modulo $p$ donc c'est le deuxième facteur qui doit valoir 0. Soit

$$a^{\frac{p-1}{2}} \equiv -1 \mod(p)$$

**Condition pour que 2 soit un carré modulo $p$**

$p$ est un nombre premier impair.
2 est un carré modulo $p$ si et seulement si $p \equiv 1 \mod(8)$ ou $p \equiv 7 \mod(8)$

Premier exemple :
Si $p = 17$, nous avons $p \equiv 1 \mod(8)$.
Nous considérons alors le produit :

$$(2.1).(2.2).(2.3).(2.4).(2.5).(2.6).(2.7).(2.8) = 2.4.6.8.10.12.14.16 = 2^8.8!$$

Nous souhaitons désormais exprimer les facteurs de ce produit par leurs représentants compris entre $-8$ et $8$
Nous avions :

$$(2).(4).(6).(8).(10).(12).(14).(16)$$

Nous aurons :

$$(2).(4).(6)(8).(-7).(-5).(-3).(-1) = (-1)^4.8!$$

Nous en déduisons :

$$2^8.8! \equiv (-1)^4.8! \mod(17)$$

soit encore $2^8 \equiv 1 \mod(17)$ ce qui, grâce au critère d'Euler, montre que 2 est bien un carré modulo 17.

Deuxième exemple :
Si $p = 23$, nous avons $p \equiv 7 \mod(8)$. $p$ s'écrit donc $p = 8k + 7$ avec $k$ entier naturel non nul, d'où $\dfrac{p-1}{2} = 4k + 3$.
Nous considérons alors le produit :

$$(2.1).(2.2).(2.3).(2.4).(2.5).(2.6).(2.7).(2.8).(2.9).(2.10).(2.11) = 2^{11}.11!$$

Comme précédemment, nous souhaitons exprimer les facteurs de ce produit par leurs représentants compris entre $-11$ et $11$
Nous avions :

$$(2).(4).(6).(8).(10).(12).(14).(16).(18).(20).(22)$$

Nous aurons :

$$(2).(4).(6)(8).(10).(-11).(-9)(-7).(-5).(-3).(-1) = (-1)^6.11!$$

Nous en déduisons :

$$2^{11}.11! \equiv (-1)^6.11! \mod(23)$$

soit encore $2^{11} \equiv 1 \mod(23)$ ce qui, grâce au critère d'Euler, montre que 2 est bien un carré modulo 23.

Preuve : Si $p \equiv 1 \mod(8)$.$p$ s'écrit donc $p = 8k+1$ avec $k$ entier naturel non nul, d'où $\dfrac{p-1}{2} = 4k$.
Nous considérons le produit :

$$(2.1).(2.2).(2.3)\ldots\left(2.\frac{p-1}{2}\right) = 2.4.6\ldots(p-1) = 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$$

Nous souhaitons ensuite exprimer les facteurs de ce produit par leurs représentants compris entre $-\dfrac{p-1}{2}$ et $\dfrac{p-1}{2}$
Nous avions :

$$(2).(4).(6)\ldots(4k).(4k+2)\ldots(8k)$$

Nous aurons :

$$(2).(4).(6)\ldots(4k).((4k+2)-p).((4k+4)-p)\ldots(8k-p)$$

ou encore, en n'oubliant pas que $p = 8k + 1$

$$(2).(4).(6)\ldots(4k).(-4k+1).(-4k+3)\ldots(-1)$$

le calcul de ce produit donne : $(-1)^{2k}\left(\frac{p-1}{2}\right)!$ soit $2^{\frac{p-1}{2}} \equiv 1 \mod(p)$ ce qui permet de conclure.
Si $p \equiv 7 \mod(8)$. $p$ s'écrit donc $p = 8k + 7$ avec $k$ entier naturel non nul, d'où $\dfrac{p-1}{2} = 4k + 3$.
Nous considérons le produit :

$$(2.1).(2.2).(2.3)\ldots\left(2.\frac{p-1}{2}\right) = 2.4.6\ldots(p-1) = 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$$

Nous souhaitons ensuite exprimer les facteurs de ce produit par leurs représentants compris entre $-\dfrac{p-1}{2}$ et $\dfrac{p-1}{2}$
Nous avions : $(2).(4).(6)\ldots(4k).(4k+2).(4k+4)\ldots(8k+6)$
Nous aurons :

$$(2).(4).(6)\ldots(4k+2).((4k+4)-p).((4k+6)-p)\ldots(8k+6-p)$$

ou encore, en n'oubliant pas que $p = 8k + 7$

$$(2).(4).(6)\dots(4k+2).(-4k-3).(-4k-1)\dots(-1)$$

le calcul de ce produit donne : $(-1)^{2k+2}\left(\frac{p-1}{2}\right)!$ soit $2^{\frac{p-1}{2}} \equiv 1 \mod(p)$ ce qui permet de conclure comme précédemment.