Ce problème d'arithmétique a été proposé par **George Gras**, qui le présente comme un lemme nécessaire qu'il a rencontré dans ses travaux de recherche.
Voici la démarche de **Jean-Claude Carréga**. Cette démarche a le mérite d'être complètement explicite. Soit p un nombre premier congru à -1 modulo 8 et soit $x, y \in \mathbb{Z}$ tels que $x^2 - py^2 = 1$. Dans $\mathbb{Z}/8\mathbb{Z}$, cette relation devient

$$\overline{x}^2 + \overline{y}^2 = 1.$$

Or modulo 8, les différentes valeurs des carrés sont 0, 1 et 4 comme le montre le tableau ci-dessous :

$\overline{x}$	0	±1	±2	±3	4
$\overline{x}^2$	0	1	4	1	0

Une somme de deux carrés peut donc, modulo 8, valoir 0; 1; 2 ou 5 et les seules facons d'obtenir 1 sont

$$1 = 1^2 + 0^2 = 0^2 + 1^2.$$

Il en résulte que l'on a soit $\overline{x} = 0$, soit $\overline{y} = 0$, ce qui montre que 8 divise x ou y. On se place maintenant dans le second cas : 8 divise y donc y est pair et puisque $x^2 - py^2 = 1$, l'entier x est impair. On cherche des entiers $u, v \in \mathbb{Z}$ tels que

$$\left(u+v\sqrt{p}\right)^2 = \pm\left(x+y\sqrt{p}\right).$$

Le signe ± est donc celui de $x+y\sqrt{p}$ et il ne pose aucun problème. Or si (x, y) est solution de $x^2 - py^2 = 1$, les couples $(\pm x, \pm y)$ aussi et l'on suppose désormais que x et y appartiennent à $\mathbb{N}$. On cherche donc $u, v \in \mathbb{Z}$ tels que

$$x+y\sqrt{p} = \left(u+v\sqrt{p}\right)^2.$$

On écarte le cas où $y = 0$: dans ce cas, $x = 1$ et l'on choisit $u = 1$ et $v = 0$. Avec $x \in \mathbb{N}$ et $y \in \mathbb{N}^*$, l'écriture

$$x+y\sqrt{p} = \left(u+v\sqrt{p}\right)^2$$

équivaut à

$$x+y\sqrt{p} = \left(u^2+pv^2\right)+2uv\sqrt{p}.$$

Or l'écriture d'un nombre réel de la forme $a+b\sqrt{p}$ avec a et b dans $\mathbb{Z}$ est unique puisque l'entier p est premier donc n'est pas un carré. Donc on cherche $u, v \in \mathbb{Z}$ tels que

$$x = u^2+pv^2 \text{ et } y = 2uv,$$

soit encore

$$x = u^2+pv^2,\ \frac{py^2}{4} = \left(u^2\right)\left(pv^2\right) \text{ et } uv > 0.$$

Ainsi, u^2 et pv^2 sont les racines de l'équation de degré 2

$$X^2 - xX + \frac{py^2}{4} = 0.0$$

Le discriminant de cette équation est

$$\Delta = x^2 - py^2 = 1$$

et les racines sont

$$\frac{x+1}{2} \text{ et } \frac{x-1}{2}.$$

Puisque x est impair, ces deux racines sont bien entières. Il faut maintenant vérifier que l'une de ces deux racines est un carré et que l'autre est le produit de p par un carré. Avant cela, remarquons que les nombres $\frac{x+1}{2}$ et $\frac{x-1}{2}$ sont consécutifs donc premiers entre eux.
La relation $x^2 - py^2 = 1$ s'écrit aussi

$$\left(\frac{x-1}{2}\right)^2\left(\frac{x+1}{2}\right)^2=\frac{py^2}{4}.$$

L'entier p divise un des deux facteurs du premier membre, disons $\dfrac{x+\varepsilon}{2}$. On a alors

$$\left(\frac{x-\varepsilon}{2}\right)^2\left(\frac{x+\varepsilon}{2p}\right)^2=\left(\frac{y}{2}\right)^2.$$

Le second membre de cette relation est un carré et les facteurs du premier membre sont premiers entre eux, donc chacun est un carré. Il existe des entiers u et v tels que

$$\frac{x-\varepsilon}{2}=u^2 \text{ et } \frac{x+\varepsilon}{2p}=v^2.$$

Les valeurs des entiers u et v cherchés sont donc

$$u=\pm\sqrt{\frac{x-\varepsilon}{2}} \text{ et } v=\sqrt{\frac{x+\varepsilon}{2p}}.$$

en choisissant le même signe pour u et v, par exemple + pour les deux.

Vérification : avec u et v trouvés précédemment,

$$\left(u+v\sqrt{p}\right)^2=\left(\sqrt{\frac{x-\varepsilon}{2}}+\sqrt{p}\sqrt{\frac{x+\varepsilon}{2p}}\right)^2,$$

soit

$$\left(u+v\sqrt{p}\right)^2=\frac{x-\varepsilon}{2}+\frac{x+\varepsilon}{2}+2\sqrt{\frac{x^2-1}{4}}=x+\sqrt{py^2}=x+p\sqrt{y}.$$