EQUATIONS DIOPHANTIENNES (*)

Jean-François BOUTOT

L'étude des équations diophantiennes est l'un des plus anciens problèmes des mathématiques : on s'y intéressait bien avant DIOPHANTE d'Alexandrie qui leur laissa son nom au 3^{e} siècle de notre ère. On appelle équation diophantienne une équation algébrique à coefficients dans $\mathbb{Z}$ dont on cherche les solutions dans $\mathbb{Z}$ comme par exemple $x^2 - 3y^2 = 2z^3$.

On généralise cette notion au cas de la recherche des solutions rationnelles d'une équation algébrique à coefficients entiers ou rationnels (on peut toujours se ramener au cas des coefficients entiers en multipliant par le dénominateur commun de tous les coefficients). L'ensemble $\mathbb{Q}$ des rationnels formant un corps, la résolution de ce type d'équations en est facilité. On peut d'ailleurs associer aux solutions rationnelles d'une équation diophantienne les solutions entières d'une autre équation diophantienne. Par exemple :

$$\begin{array}{lll} x^2 + y^2 = 1 & \text{et} & X^2 + Y^2 = T^2 \\ (x, y) \in \mathbb{Q}^2 & & (X, Y, T) \in \mathbb{Z}^3 \end{array}$$

puisque si (x, y) est solution rationnelle de la première on peut écrire $x = X/T$ et $y = Y/T$ ce qui conduit au deuxième système (dit homogène).

Dans ce qui suit nous nous intéresserons aux équations diophantiennes rationnelles à deux inconnues : $f(x, y) = 0$. Résoudre $f(x, y) = 0$ s'interprète comme la recherche sur une courbe algébrique du plan $\mathbb{R}^2$ des points à coordonnées rationnelles (ou points rationnels). Pour une bonne approche du problème on commence par voir ce qui se passe pour f de degré petit.

Le DEGRÉ 1 : Cas des droites

C'est un problème classique d'arithmétique. On sait qu'il y a une infinité de solutions et que quand on en connaît une (x_0, y_0) alors en posant $f(x, y) = ax + by + c = 0$; $(a, b, c,) \in \mathbb{Z}^3$ on a : $f(x, y) - f(x_0, y_0) = a(x - x_0) + b(y - y_0) = 0$ donc toutes les autres sont de la forme

$$\begin{aligned} x &= x_0 + tb \\ y &= y_0 - ta \end{aligned}$$

où $t \in \mathbb{Q}$.

(*) Rédaction d'après les notes de Jean LEFORT, d'une conférence APM - IREM, donnée le 15 mars 1989

Le DEGRÉ 2 : Cas des coniques

Le problème se complique puisqu'il y a des cas où il n'y a pas de solution comme cela est manifeste, par exemple, pour l'équation $x^2 + y^2 + 1 = 0$ qui n'a pas de solutions réelles donc a fortiori de solutions rationnelles.

Il est facile de voir que si il y a une solution rationnelle alors il y en a une infinité. Pour comprendre pourquoi cela a lieu, prenons l'exemple du cercle $x^2 + y^2 = 1$ qui admet le point rationnel $p_0(-1, 0)$. On fait passer par p_0 une droite de pente t rationnelle. Il est clair que le deuxième point d'intersection de cette droite avec le cercle a des coordonnées rationnelles qui valent

$$x = \frac{1 - t^2}{1 + t^2}$$
$$y = \frac{2t}{1 + t^2} \qquad t \in \mathbb{Q}$$

Dans le cas présent, comme il a été signalé initialement, il aurait été équivalent de chercher les solutions entières de l'équation homogène associée : $X^2 + Y^2 = Z^2$, ce qui revient à résoudre le problème des triplets de nombre pythagoriciens (nombres entiers pouvant être les côtés d'un triangle rectangle). Alors le même raisonnement conduit à :

$$X = a^2 - b^2$$
$$Y = 2ab$$
$$Z = a^2 + b^2$$

avec a et b entiers et premiers entre eux.

Le raisonnement que nous venons de faire pour le cercle s'applique tel quel à n'importe quelle conique. Ou bien elle n'a pas de points rationnels, ou bien elle en a un p_0, et une droite de pente t ($\in \mathbb{Q}$) passant par p_0 recoupe la conique en un point rationnel P(t). Toute la question est de savoir si il y a ou non au moins un point rationnel sur la conique. Ce problème a été résolu par LEGENDRE. On se ramène par changement de repère à l'équation homogène

$$AX^2 + BY^2 + CZ^2 = 0 \qquad (A, B, C) \in \mathbb{Z}^3.$$

Pour que l'équation ait une solution rationnelle il faut

1) qu'il existe une solution réelle
2) qu'il existe une solution modulo A
une solution modulo B
et une solution modulo C
3) qu'il existe une solution modulo 8

Il est facile de voir qu'il n'y a qu'un nombre fini de triplets (X, Y, Z) à tester. Cette règle est un cas particulier du principe de HASSE.

Le DEGRÉ 3 : Cas des cubiques

Nous distinguerons deux cas selon qu'il s'agit d'une cubique singulière (c'est-à-dire présentant un point double ou un point de rebroussement) ou non.

1. Cas des cubiques singulières

Considérons l'exemple de la strophoïde d'équation

$$x(x^2+y^2) = x^2 - y^2$$

qui admet un point double ordinaire (c'est-à-dire à tangentes distinctes) à l'origine. Rappelons que les tangentes à l'origine sont données par les termes de plus bas degré, ici $x^2 - y^2$ soit $(x-y)(x+y) = 0$.

Coupons la strophoïde par une droite de pente rationnelle passant par le point double. Nous obtenons alors le paramétrage

$$x = \frac{1-t^2}{1+t^2}$$
$$y = \frac{t(1-t^2)}{1+t^2}$$

qui donne ainsi une infinité de points rationnels.

Une étude analogue pour la cissoïde d'équation $x(x^2+y^2) = y^2$ qui admet un point de rebroussement à l'origine conduit au paramétrage

$$x = \frac{t^2}{1+t^2}$$
$$y = \frac{t^3}{1+t^2}.$$

D'une façon générale une cubique n'admet qu'au plus un point singulier et on démontre que si le point singulier existe c'est un point à coordonnées rationnelles (toujours dans le cas où les coefficients de l'équation sont rationnels).

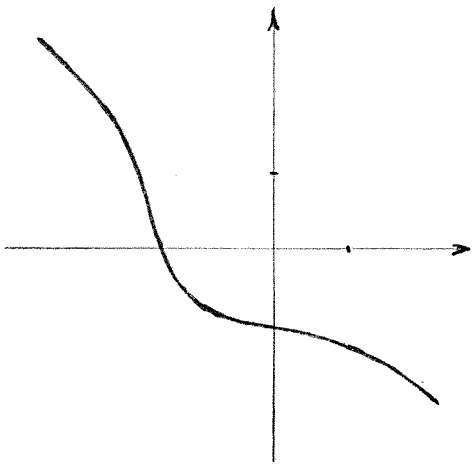
2. Cas des cubiques non singulières

Une cubique a toujours des points réels mais pas toujours des points rationnels. SELMER a donné en 1951 l'exemple de

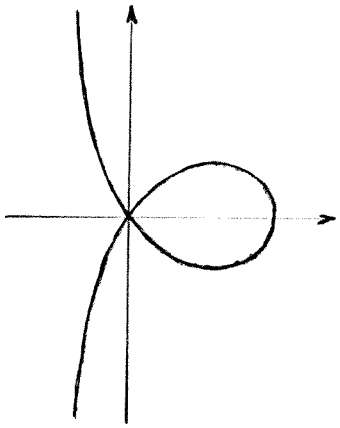
$$3X^3 + 4Y^3 + 5Z^3 = 0 \quad \text{(équation homogène associée)}$$

qui malgré l'existence de solution modulo n pour tout n n'admet pas de solution entière. Il n'y a donc pas de points rationnels sur la cubique

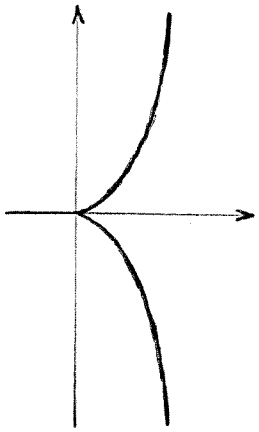
$$3x^3 + 4y^3 + 5 = 0$$



Cubique de Selmer



Strophoïde droite



Cissoïde droite

Figure 1

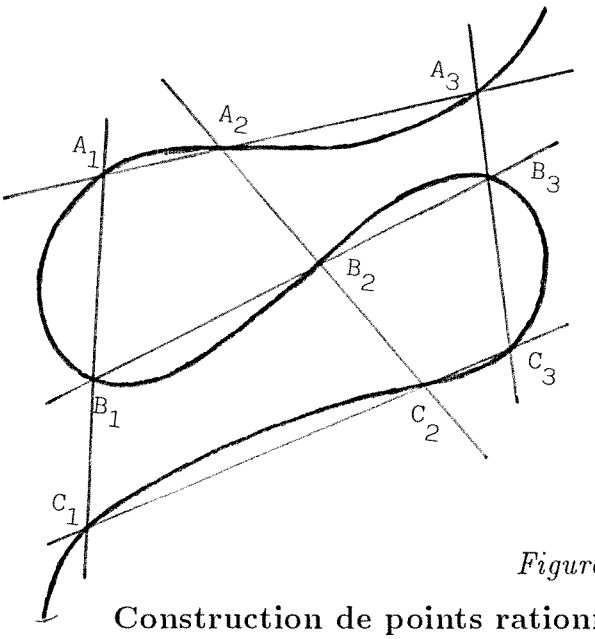
Pour aller plus loin, nous avons besoin de quelques résultats.

Théorème de Lamé. Soit C une cubique. Soient $A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3$ neuf points tels que

$A_1A_2A_3$ soient alignés
$B_1B_2B_3$ soient alignés
$C_1C_2C_3$ soient alignés
$A_1B_1C_1$ soient alignés
$A_2B_2C_2$ soient alignés.

Alors les points A_3B_3 et C_3 sont aussi alignés (fig. 2 ci-dessous).

Loi de groupe sur une cubique. En se plaçant dans l'espace projectif complexe on démontre qu'une cubique admet neuf points d'inflexions. On en choisit un comme origine Ω et on associe à deux points P et Q de la cubique le point R tel que si la droite (PQ) recoupe en T la cubique, alors $T\Omega$ recoupe en R la cubique. Une autre façon de voir est de dire que trois points alignés ont une somme nulle (égale à Ω). On définit ainsi une loi interne sur l'ensemble des points de la cubique $(P+Q=R)$. Cette loi est commutative, admet Ω comme élément neutre, l'opposé de P étant le point P' tel que (PP') passe par Ω. Le théorème de LAMÉ traduit l'associativité de cette loi qui est donc une loi de groupe.



En effet, prenons $B_2 = \Omega$ comme origine (fig. ci-contre). Alors

$$\begin{aligned}(A_2 + A_1) + B_1 &= -A_3 + B_1 \\ &= -A_3 - B_3 = C_3 \\ A_2 + (A_1 + B_1) &= A_2 - C_1 \\ &= -C_2 - C_1 = C_3\end{aligned}$$

Figure 2

Construction de points rationnels à partir de l'un d'eux :

Soit P un point rationnel. On peut définir $2P, 3P \ldots nP$ de la façon suivante : la tangente en P recoupe la cubique en $-2P$. $2P$ est le point aligné avec Ω (point d'inflexion choisi comme origine) et $-2P$ (voir fig. 3). Puis avec $P+2P$ on construit $3P$ etc...

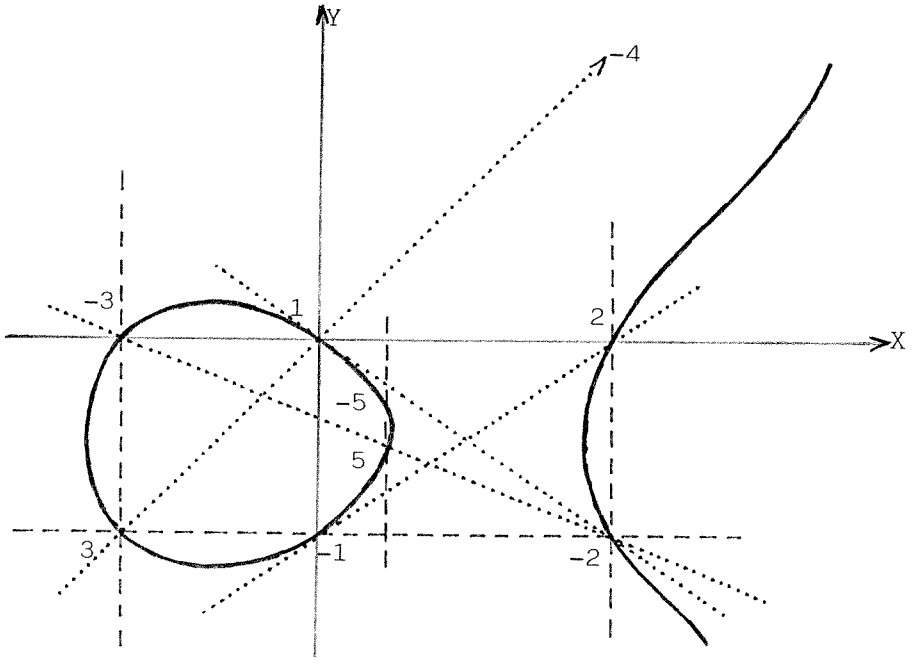


Figure 3

Cubique $y^2 = x^3 + px + q$.

On choisit comme origine le point d'inflexion à l'infini dans la direction de Oy.

On démontre que nP est rationnel ce qui permet d'affirmer que l'ensemble des points rationnels forme un sous-groupe abelien : $C(\mathbb{Q})$. En 1922 MORDELL

démontra :

Théorème de Mordell : Le groupe des points rationnels d'une cubique est de type fini, ce qui veut dire qu'il existe n points $P_1, P_2 \dots P_n$ de $C(\mathbb{Q})$ tels que pour tout P de $C(\mathbb{Q})$ il existe des m_i dans $\mathbb{Z}$ avec :

$$P = m_1 P_1 + m_2 P_2 + \cdots m_n P_n.$$

Le groupe $C(\mathbb{Q})$ est de la forme $\mathbb{Z}^r \oplus$ groupe abelien fini. $\mathbb{Z}^r$ correspond aux points P_i d'ordre infini tandis que le groupe fini, dit groupe de torsion, correspond aux points P_i d'ordre fini (c'est-à-dire pour lesquels il existe n tel que $nP_i = \Omega$).

Ce n'est qu'en 1976 que MAZUR donna la forme du groupe de torsion. Il n'y a que 15 possibilités :

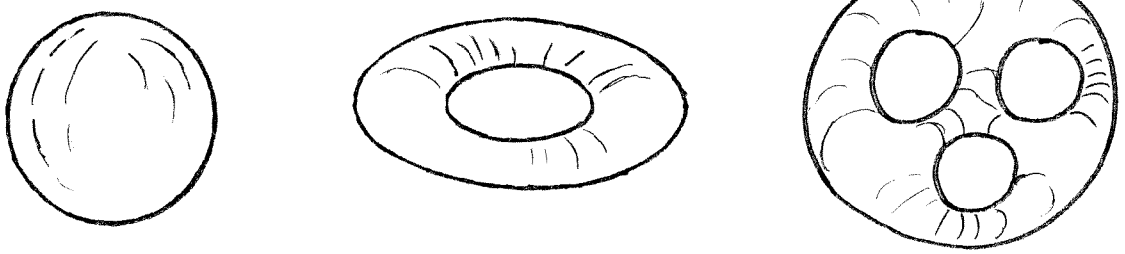
$$\mathbb{Z}/m\mathbb{Z} \text{ avec } m \leq 10 \text{ ou } m = 12$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ avec } n \leq 4.$$

Quand au rang r, on a fait beaucoup de conjectures en étudiant les solutions modulo un nombre premier p. Les exemples suivants montrent la grande variété des possibilités :

* FERMAT : $X^3 + Y^3 = Z^3$ alors $C(\mathbb{Q}) = \{(1,-1,0),(1,0,1),(0,1,1)\}$
$= \mathbb{Z}/3\mathbb{Z}$.
* EULER : $X^3 + Y^3 = 3Z^3$ alors $C(\mathbb{Q}) = \{(1,-1,0)\}$
$X^3 + Y^3 = 2Z^3$ alors $C(\mathbb{Q}) = \{(1,-1,0),(1,1,1)\}$.
* TATE : $y^2 + y = x^3 - x$ alors $C(\mathbb{Q}) = \mathbb{Z}$ engendré par $(0,0)$.
Il n'y a pas de torsion.

Approche du cas général

• Il ressort de l'étude précédente que le degré n'est pas l'invariant fondamental. Il faut aussi tenir compte des singularités. L'invariant qui en tient compte est le **genre**. Pour définir le genre d'une courbe plane, il faut la considérer comme une surface réelle plongée dans un espace de dimension 4. A cet effet on considère le plan projectif complexe $\mathbb{P}^2_{\mathbb{C}}$ qui est de dimension 2 sur $\mathbb{C}$ mais 4 sur $\mathbb{R}$. La courbe C est alors une surface dans cet espace et on s'intéresse à son genre (c'est-à-dire schématiquement au nombre de trous analogues à celui d'un tore qui est de genre 1).



sphère : genre 0 — tore : genre 1 — surface de genre 3

Figure 4

• Reprenons l'exemple de la droite. Dans $\mathbb{P}^2_{\mathbb{C}}$ elle correspond à un plan auquel on a adjoint un point à l'infini ce qui en fait l'analogue d'une sphère de genre 0.

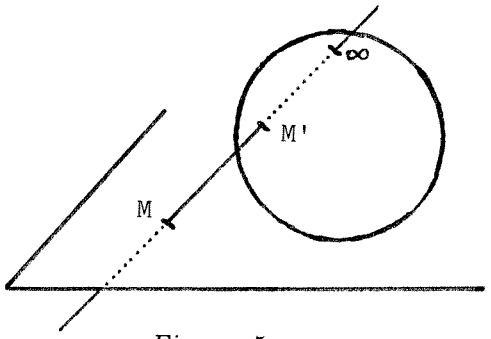


Figure 5

Bijection entre les points M d'un plan
et les points M^0 d'une sphère tangente à ce plan.

Mais ce sera également le cas quand on peut établir une "*bijection*" entre une droite et la courbe C comme cela a été fait pour les coniques et les cubiques singulières.

Dans le cas des cubiques singulières on n'avait pas réellement une bijection (et c'est la raison de la présence des guillemets). Mais il existe une méthode : l'éclatement, qui permet de construire une "*vraie*" bijection.

• Nous allons maintenant démontrer que le genre d'une cubique non singulière est 1. Pour cela considérons une fonction f méromorphe et doublement périodique sur $\mathbb{C}$ (soient 1 et τ ses périodes). On sait que ce sont des fonctions elliptiques telles que la fonction $\wp(z)$ de WEIERSTRASS définie par :

$$\wp(z) = \frac{1}{z^2} + \Sigma_{w \in \bigwedge^*} [\frac{1}{(z-w)^2} - \frac{1}{w^2}]$$

où $\bigwedge = \mathbb{Z}_1 \oplus \mathbb{Z}_\tau$ est l'ensemble des nœuds du quadrillage engendré par 1 et τ, et $\bigwedge^*$ cet ensemble privé de $(0,0)$.

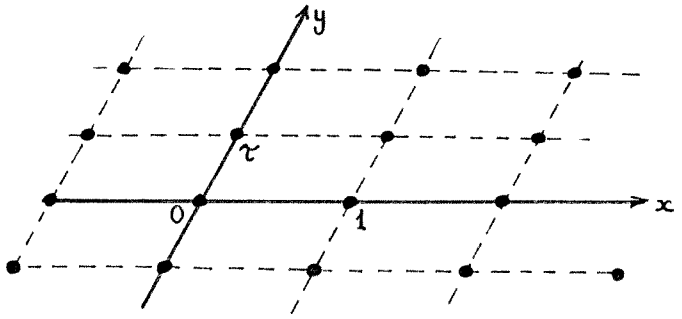


Figure 6

éléments de $\bigwedge$

Par dérivation on a : $\wp'(z) = \Sigma_{w \in \bigwedge} \frac{-2}{(z-w)^3}$ et on peut voir que $\wp(z)$ satisfait l'équation différentielle :

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

où

$$g_2 = 60\Sigma_{w\in\bigwedge^*}\frac{1}{w^4}$$

et

$$g_3 = 140\Sigma_{w\in\bigwedge^*}\frac{1}{w^6}.$$

En posant $\wp' = y$ et $\wp = x$ on trouve une cubique. On sait que toutes les fonctions elliptiques sont engendrées par $\wp$ et $\wp'$ et forment ainsi un corps. La procédure précédente permet de mettre en bijection l'ensemble $\mathbb{C}/\bigwedge$ et la courbe $C_{\mathbb{C}}$ d'équation $y^2 = 4x^3 - g_2 - g_3$. Or $\mathbb{C}/\bigwedge$ s'identifie sans problème à un tore (de genre 1) en "*recollant*" les côtés opposés du parallélogramme construit sur 1 et τ.

Figure 7

La loi de groupe qui a été mise en évidence sur la cubique n'est rien d'autre que l'addition dans $\mathbb{C}$.

• En genre supérieur ou égal à 2, MORDELL, en 1922, à partir de nombreux exemples, conjecture qu'il n'y a qu'un nombre fini de points rationnels. Ce n'est qu'en 1983 que G. FALTINGS démontre cette conjecture. Il n'est pas question dans le cadre de cet exposé de présenter la démonstration de FALTINGS, démonstration qui fait appel à toutes les ressources de la géométrie algébrique telle que l'a reformulée GROTHENDIECK.

Donnons toutefois quelques renseignements sur la façon de calculer le genre d'une courbe :
Si $f(x, y) = 0$ définit une courbe C non singulière de degré d alors son genre g est :

$$g = \frac{(d-1)(d-2)}{2}.$$

Si la courbe C possède n points singuliers ordinaires (point double à tangentes distinctes ou points de rebroussement) alors le genre vaut

$$g = \frac{(d-1)(d-2)}{2} - n.$$

On fera cependant attention que le décompte doit se faire dans le plan projectif complexe. C'est ainsi que l'**astroïde** d'équation :

$$(x^2 + y^2 - 1)^3 + 27x^2y^2 = 0$$

possède :

4 points singuliers réels (points de rebroussement);
4 points doubles complexes $((\pm i, \pm i))$;
2 points doubles à l'infini.

ce qui conduit pour cette courbe de degré 6 à un genre égal à 0. On aurait pu s'en douter autrement quand on connaît la représentation paramétrique de l'astroïde :

$$x = \cos^3 \theta$$
$$y = \sin^3 \theta$$

qui met en évidence la "*bijection*" avec la droite par l'intermédiaire de θ (et d'un cercle).

• Et FERMAT dans tout ça? On sait que FERMAT avait annoncé en marge de son exemplaire de l'arithmétique de DIOPHANTE, avoir trouvé une démonstration simple de l'inexistence de solutions entières non triviales de l'équation

$$x^n + y^n = z^n$$

pour $n \geq 3$ (les solutions triviales sont du type $(0, a, a)$). Or pour $n \geq 4$, le genre de $X^n + Y^n = Z^n$ vaut $\big((n-1)(n-2)\big)/2$ qui est supérieur ou égal à 3. Le théorème de FALTINGS assure que cette équation n'a qu'un nombre fini de solutions entières avec X, Y et Z premiers entre eux. Ceci ne résoud pas tout à fait la question mais laisse de sérieux espoirs.

On sait qu'on a l'habitude de décomposer le problème de FERMAT en deux cas :
— le 1er cas qui dit que l'équation $x^p + y^p = z^p$ n'a pas de solution en entiers non divisibles par p,
— le 2ème cas qui dit que l'équation n'a pas de solution en entiers dont l'un au moins est divisible par p.

On conjecture que le 1er cas est vrai car si il y avait une solution (α, β, γ) avec $\alpha^p + \beta^p = \gamma^p$ la cubique $y^2 = x(x - \alpha^p)(x - \beta^p)$ pourrait ne pas exister.

En fait le problème de FERMAT a donné lieu à de très nombreuses recherches dans toutes les directions et on peut signaler que c'est grâce à lui que KUMMER a construit ses "nombres idéaux" qui ont conduit plus tard à la notion d'idéal d'anneaux.

On a montré récemment qu'il existait une infinité de nombres premiers pour lesquels le 1er cas est vrai, ce qui ne veut pas dire qu'il est vrai pour tout p même si on sait qu'il est vrai pour $p \leq 253\ 747\ 889$.