Contre-exemples au principe de Hasse

Bruno Winckler

15 octobre 2011

Le théorème de Hasse-Minkowski énonce que si une forme quadratique définie sur le corps des rationnels représente 0 dans tout complété de $\mathbb{Q}$ (*i.e.* dans tout corps p-adique $\mathbb{Q}_p$ et dans $\mathbb{R}$), alors elle représente 0 dans $\mathbb{Q}$, et réciproquement ; ce résultat est démontré dans le *cours d'arithmétique* de Jean-Pierre Serre, par exemple. Si on remplace une forme quadratique par un polynôme à plusieurs indéterminés quelconque, ce théorème n'est plus vrai *a priori*, et je me propose de fournir quelques exemples où il est en défaut. Je précise que je n'ai rien inventé. Les exemples se veulent élémentaires, ainsi je ne traiterai pas, par exemple, le cas de la courbe de Selmer donnée par l'équation $4x^3 + 4y^3 + 5z^3 = 0$, même si la méthode de résolution de ce problème est intéressante (on fait de l'arithmétique dans l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{2})$). Keith Conrad traite cet exemple dans *Selmer's example*, disponible sur Internet.

En fait, les exemples que je vais traiter font intervenir des polynômes à coefficients entiers, et ont des solutions modulo tout entier non nul. Ils ne contredisent pas tous le principe de Hasse, puisque certaines des hypothèses requises ne seront pas toujours présentes, mais chaque exemple illustre quelque chose d'autre.

On sait que tout entier positif s'écrit comme somme de quatre carrés : c'est aussi prouvé dans le cours de Jean-Pierre Serre, grâce au théorème de Hasse-Minkowski ; d'autres méthodes utilisant les quaternions existent, et à cet effet le cours de *théorie algébrique des nombres* de Pierre Samuel est un atout précieux. Ceci étant dit, voici un exemple proche de ce qu'on cherche mais qui n'a pas de solution réelle ; je le mets parce que je le trouve *rigolo* :

Proposition 1 *L'équation $x^2+y^2+z^2+t^2 = -1$ a des solutions modulo tout entier non nul, mais n'a pas de solution rationnelle.*

Preuve. En effet, soit n un entier non nul. On peut représenter $n-1$ comme une somme de quatre carrés, et on obtient le résultat voulu en réduisant modulo n. Il est clair qu'il n'y a pas de solution rationnelle, ni même réelle. □

Je vous l'accorde, ce n'est pas un exemple tout à fait élémentaire, vu qu'il invoque un résultat plus difficile et que je n'ai pas démontré. On va donc reprendre, mais en douceur :

Proposition 2 (dû à Ravi Boppana) *L'équation $(2x-1)(3x-1) = 0$ a des solutions modulo tout entier non nul, mais n'a pas de solution entière.*

Preuve. Seule la première assertion mérite d'être démontrée. Soit n un entier. S'il n'est pas pair, alors 2 est inversible modulo n, donc $2x - 1 = 0$ a une solution modulo n, à savoir l'inverse de 2 modulo n. De plus, si n n'est pas un multiple de 3, par le même argument, $3x - 1 = 0$ a une solution après réduction. À présent, si n ne rentre pas dans les cas précédents, donc est un multiple de 6, alors on utilise le lemme des restes chinois pour se ramener à la résolution de l'équation de la proposition modulo une puissance de 2, une puissance 3 et modulo un entier étranger à 6. Modulo la puissance de 2 (qui n'est pas un multiple de 3) et modulo la puissance de 3 (qui n'est pas un multiple de 2), on a une solution par le raisonnement qui précède. Modulo l'entier premier à 6, les deux situations ci-dessus se réalisent, je vous laisse donc choisir ce que vous préférez. □

Légèrement plus sophistiqué, mais toujours dans ce registre :

Proposition 3 (dû à Felipe Voloch) *L'équation $x^2 + 23y^2 = 41$ a des solutions modulo tout entier non nul, mais n'a pas de solution entière.*

Preuve. On peut vérifier que $\left(\frac{1}{3}, \frac{4}{3}\right)$ est une solution rationnelle. Après multiplication par neuf et réduction modulo un entier premier à 3, on obtient une solution équation modulo n qu'on sait résoudre. Mais $\left(\frac{9}{4}, \frac{5}{4}\right)$ est aussi une solution rationnelle, ce qui fournit une solution dans le cas impair. Comme précédemment, le lemme chinois permet de résoudre le problème modulo tout entier non nul (remarque : on peut conclure sans le cas impair : si on réduit modulo une puissance de 3, on peut toujours trouver une solution avec $x = 0$). Par contre, il n'y a pas de solution entière : s'il existait des entiers x et y solutions entières, alors la réduction modulo 4 fournirait l'égalité $x^2 - y^2 = 1$, ce qui impose que x^2 est congru à 1 modulo 4, et que y^2 est un multiple de 4. En écrivant $y = 2k$, cette équation se ramène à la résolution de

$$x^2 + 92k^2 = 41.$$

Si k est non nul, alors $x^2 + 92k^2$ est strictement supérieur à 41, ce qui impose $k = 0$. Cependant, $x^2 = 41$ n'a pas de solution, donc l'équation n'a pas de solution entière. □

Enfin, *the last but not the least*, je contredis le principe de Hasse :

Proposition 4 (dû à Qiaochu Yuan) *L'équation $(x^2-2)(x^2-17)(x^2-34) = 0$ a des solutions modulo tout entier non nul, mais n'a pas de solution rationnelle.*

Comme il est clair que cette équation a des solutions réelles, et que les solutions modulo tout entier (donc en particulier modulo toute puissance d'un nombre premier) induisent des solutions p-adiques, le principe de Hasse est bien contredit. Le choix de 2 et 17 sera clair au fil de la démonstration.

Preuve. Montrons qu'elle a une solution modulo tout nombre premier. Si on réduit modulo 2 ou modulo 17, c'est facile (en fait, modulo 17, 2 est un carré, de racine carrée 6 par exemple ; il y a aussi la solution triviale 0). Réduisons donc modulo un autre nombre premier p. Montrer que cette équation a une solution modulo p revient à dire que soit 2, soit 17, soit 34 est un carré modulo p. Comme le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $\{\pm 1\}$, et que $34 = 17 \cdot 2$, on en déduit sans trop de difficulté qu'au moins l'une de ces quantités est un carré (une ou les trois d'entre elles, en fait), et donc que l'équation a une solution modulo p. On peut alors induire des solutions modulo toute puissance d'un nombre premier, grâce au lemme suivant :

Lemme 5 (Lemme de Newton p-adique simplifié) *Soit P un polynôme à coefficients entiers. S'il existe un entier a tel que, pour un certain entier n et un autre entier k strictement inférieur à la moitié de n :*

$$P(a) \equiv 0 \mod p^n, P'(a) \equiv 0 \mod p^k \text{ et } P'(a) \not\equiv 0 \mod p^{k+1},$$

alors il existe un entier a_0 tel que

$$P(a_0) \equiv 0 \mod p^{n+1}, P'(a_0) \equiv 0 \mod p^k \text{ et } P'(a) \not\equiv 0 \mod p^{k+1}$$

et $a \equiv a_0 \mod p^{n-k}$.

La moralité de ce lemme est qu'il permet de remonter des solutions modulo p^n en des solutions modulo p^{n+1}. Admettons-le pour un instant, et voyons comment l'utiliser : notons P le polynôme qui définit le membre de gauche de l'équation.

Cas des puissances de 17. On a $P'(6) \equiv 2 \cdot 6 \cdot 6^2 \cdot 6^2 \not\equiv 0 \mod 17$, donc on peut utiliser le lemme de Newton (avec $k = 0$) pour obtenir une solution modulo 17^2, et en fait modulo toute puissance de 17 en réitérant. À ce stade, le choix de 17 se justifie par le fait que 2 devait être un carré modulo le second nombre premier choisi pour définir P, sinon on n'a que 0 comme solution ici, et on ne peut pas relever notre solution à l'aide du lemme de Newton (c'est pourquoi 3 n'aurait pas marché, par exemple).

Cas des puissances p, $p \neq 2, 17$. Soit x une solution de l'équation modulo p. Comme x est la racine carrée de 2, 17 ou 34 qui sont tous inversibles modulo p, x est lui-même inversible. Imaginons que x soit une racine carrée de 2. Alors $P'(x) \equiv 2x \cdot (x^2 - 17)(x^2 - 34) \not\equiv 0 \mod p$, donc on peut utiliser le lemme de Newton (avec $k = 0$) pour obtenir une solution modulo p^2, puis modulo toute puissance de p en réitérant. On conclut de la même manière si x est une racine carrée de 17 ou 34, l'important étant que seul un terme de P' ne s'annule pas.

Cas des puissances de 2. Ce cas est plus délicat, car $P'(x) \equiv 0 \mod 2$ pour tout x entier. On raisonne donc modulo 8 pour utiliser le lemme de Newton, et on doit vérifier à la main qu'il y a des solutions modulo 4 : c'est le cas, car modulo 4, cette équation s'écrit $(x^2 - 2)^2(x^2 - 1) = 0$, qui a pour solutions 1 et -1. Modulo 8, l'équation est encore une fois très simple, puisque qu'elle s'écrit de la même manière, et a les mêmes solutions 1 et -1, mais aussi 3 et -3. Alors, comme $P'(x) \equiv 2x(x^2 - 2)^2 \mod 4$, et qu'alors $P'(1) \equiv 2 \cdot (-1)^2 \not\equiv 0 \mod 4$, on peut utiliser le lemme de Newton (avec $k = 1$) pour en déduire une solution modulo 2^4, et modulo toute puissance de 2 supérieure. Ici, on voit que le fait que 17 soit congru à 1 modulo 8 est crucial, c'est pourquoi 7 n'aurait pas marché, par exemple.

Il nous reste à prouver le lemme : prenons a_0 de la forme $a + p^{n-k}z$ avec z un entier. D'après la formule de Taylor, on a $P(a_0) = P(a) + p^{n-k}zP'(a) + p^{2n-2k}b$ avec b un entier. Comme $P(a) = p^n c$ et $P'(a) = p^k d$ pour c un entier, et d un entier premier à p, on peut choisir z de sorte que $c + zd$ soit divisible par p (en prenant $z \equiv -cd^{-1} \mod p$). Alors, $P(a_0) = p^n(c + zd) + p^{2n-2k}b \equiv 0 \mod p^{n+1}$ car $2n - 2k > n$. La formule de Taylor appliquée à P' prouve immédiatement que $P'(a_0) \equiv 0 \mod p^k$ et $P'(a_0) \not\equiv 0 \mod p^{k+1}$. □

Pour produire un exemple qui contredit le principe de Hasse, on a utilisé un polynôme réductible. C'est normal, en fait, on peut en effet démontrer le résultat suivant :

Proposition 6 *Si P est un polynôme à coefficients entiers irréductible de degré strictement supérieur à 1, alors il existe un entier p tel que l'équation $P(x) = 0$ n'ait pas de solution modulo p.*

Ce résultat nécessite quelques connaissances de théorie algébrique des nombres et de théorie de Galois. Il y a même une infinité de nombres premiers p qui conviennent.

Preuve. Soit G le groupe de Galois sur $\mathbb{Q}$ du polynôme P (*i.e.* de son corps de décomposition). Si le polynôme est irréductible, alors G agit transitivement sur les racines de P, et on déduit qu'il existe une classe de conjugaison de G sans point fixe (**à détailler**). Soit p un nombre premier tel que Frob_p soit égal à la classe de conjugaison en question ; il en existe d'après le théorème de densité de Chebotarev. En réduisant modulo ce nombre premier p, on voit que P n'a pas de racine : une telle racine serait un point fixe du Frobenius en p. □