Autour d'un résultat élémentaire

M. Tibouchi

22 mai 2004

Résumé

Comme promis, mais avec un certain retard, je propose ici une solution propre à l'un des exercices du 21 janvier, avec en prime quelques remarques culturelles s'y rapportant. Tous les commentaires, demandes d'éclaircissements, corrections, remarques orthographiques ou autres, sont les bienvenus.[1]

1 Chose promise, chose due.

Il s'agissait de montrer que pour tout polynôme f non constant à coefficients entiers, il existe une infinité de nombres premiers p tels que f ait une racine modulo p. Posons $a = f(0)$, qu'on peut bien sûr supposer non nul, et $g(X) = f(aX)$. Tous les coefficients de g sont divisibles par a, donc on peut écrire $g(X) = a \cdot g_0(X)$, avec g_0 polynôme à coefficients entiers, de même degré que f, et vérifiant $g_0(0) = 1$. Il suffit de montrer que l'ensemble des nombres premiers modulo lesquels g_0 a une racine est infini.

Supposons par l'absurde qu'il n'y en ait qu'un nombre fini, et notons m leur produit. Comme le polynôme $g_0(mX)$ n'est pas constant, il prend sur $\mathbf{Z}$ une valeur entière autre que ± 1, et il existe un entier x et un nombre premier ℓ tels que $\ell | g_0(mx)$. Alors g_0 a en particulier une racine modulo ℓ, donc $\ell | m$. Mais alors :

$$g_0(mx) \equiv g_0(0) \equiv 1 \pmod{\ell}$$

qui est la contradiction recherchée.

On n'a fait, finalement, que tirer un peu sur la corde de la preuve d'Euclide qu'il y a une infinité de nombres premiers. Et il est assez remarquable qu'on puisse obtenir autant avec si peu de moyens, car les résultats analogues plus précis sont considérablement plus difficiles. [2]

[1] Je remercie en particulier Gaëtan Chenevier, Cédric Pépin et Alexandre Pilkiewicz pour leur lecture et leurs précieuses remarques.

[2] Cependant, contrairement à ce qu'indiquait une version antérieure de cette note, le résultat selon lequel pour tout f, il existe une infinité de nombres premiers p modulo lesquels f est *scindé* (i.e. le fait que $\mathrm{Spl}(f)$ est infini, avec les notations du paragraphe 3) est encore élémentaire, même s'il requiert un attirail un peu plus fourni. En voici une démonstration, suivant un exercice proposé par Gaëtan Chenevier en TD d'algèbre.

Soit $\alpha_1, \ldots, \alpha_n$ les racines de f dans $\mathbf{C}$, et $k = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ son corps de décomposition. D'après le

2 Les cas euclidiens du théorème de la progression arithmétique.

Pour donner une idée, le résultat précédent permet de montrer facilement, en considérant pour f le polynôme cyclotomique Φ_n, qu'il existe une infinité de nombres premiers congrus à 1 modulo n. Esquissons rapidement la preuve (voir un des exercices du 28 janvier). Il suffit de montrer, grâce à ce qui précède, qu'à un nombre fini d'exceptions près, si Φ_n a une racine modulo un certain nombre premier p, alors $p \equiv 1 \pmod{n}$. On peut en fait voir que c'est le cas dès que p ne divise pas n. En effet, soit x une racine de Φ_n modulo p. On a alors, par le petit théorème de Fermat et le fait[3] que $\Phi_n | X^n - 1$:

$$x^n \equiv x^{p-1} \equiv 1 \pmod{n}$$

donc si l'on note d le PGCD de n et $p-1$, $x^d \equiv 1 \pmod{n}$. Si $d = n$, on a gagné. Sinon, x est racine modulo p de $X^d - 1$, donc de l'un des $\Phi_{d'}$ pour $d' | d$. Mais alors x est racine au moins double de $X^n - 1$, donc est racine de son polynôme dérivé nX^{n-1}. Or, puisque p est premier à n, ce polynôme n'a que la racine 0 modulo p, ce qui conclut.

D'un autre côté, montrer que pour n impair il existe une infinité de nombres premiers congrus à 2 modulo n nécessite un attirail beaucoup plus élaboré, et en tout cas beaucoup plus d'efforts. C'est à peu près aussi dur que de montrer le théorème général, dû à Dirichlet, selon lequel pour tous a, b premiers entre eux, il existe une infinité de nombres premiers de la forme $ak + b$. Le problème de la rue d'Ulm en 1993 présentait une preuve basée entièrement sur des outils de prépa, mais il faut un peu s'accrocher pour le rédiger d'un bout à l'autre. Les preuves habituelles sont plus courtes, mais utilisent quelques notions d'analyse complexe qui relèvent plutôt du programme de licence.

D'ailleurs, c'est une question intéressante de rechercher pour quels couples (a, b) on peut arriver à montrer le théorème de Dirichlet par la méthode élémentaire exposée plus haut. Il se trouve qu'on peut donner un sens précis à la question, et qu'on sait y répondre depuis peu : Murty a montré en 1988 qu'une condition nécessaire et suffisante était que $b^2 \equiv 1 \pmod{a}$. Keith Conrad en propose une présentation de la preuve dans l'exposé <http://www.math.uconn.edu/~kconrad/blurbs/dirichleteuclid.pdf>.

3 Le théorème de Čebotarev.

Il est intéressant de remarquer que la preuve du fait que ce cas-ci est en fait le seul accessible par la méthode élémentaire « à la Euclide » utilise le théorème vraiment

théorème de l'élément primitif, il existe x dans l'anneau $A = \mathbf{Z}[\alpha_1, \ldots, \alpha_n]$ tel que $k = \mathbf{Q}(x)$. On a donc des polynômes $g_1, \ldots, g_n \in \mathbf{Q}[X]$ tels que $\alpha_i = g_i(x)$. Si l'on note N le ppcm de leurs dénominateurs, on a alors $A[1/N] = \mathbf{Z}[1/N, x]$. Soit $u \in Z[X]$ le polynôme minimal de x. Il existe une infinité de nombres premiers p modulo lesquels u a une racine, ce qui revient à dire qu'il existe un morphisme d'anneaux $\mathbf{Z}[X] \to \mathbf{Z}/p\mathbf{Z}$. Mais alors pour tout tel $p > N$, il existe un morphisme d'anneau $\mathbf{Z}[1/N, x] \to \mathbf{Z}/p\mathbf{Z}$, et donc a fortiori $A \to \mathbf{Z}/p\mathbf{Z}$. Mais l'existence d'un tel morphisme signifie exactement que f est scindé modulo p : d'où le résultat.

[3] On rappelle que $X^n - 1 = \prod_{d|n} \Phi_d$.

profond et vraiment difficile qui prolonge naturellement le petit résultat de notre exercice, j'ai nommé le théorème de Čebotarev. C'est un théorème qu'il est utile d'avoir en tête, même sans savoir le prouver, parce qu'il permet de décider en un rien de temps un grand nombre de questions du type de celles qu'on a posées ici. Et surtout, c'est un résultat très beau et très satisfaisant. Je vais donc essayer d'introduire ici rapidement ce qu'il faut pour au moins l'énoncer.

La première idée, c'est qu'en plus d'une information « qualitative » sur l'existence de nombres premiers où un certain polynôme a des racines, le théorème de Čebotarev va apporter une information « quantitative », en indiquant en un certain sens la proportion de nombres premiers qui va marcher. Le sens précis est celui de densité : si A est un ensemble de nombres premiers, on dit que A a une densité lorsque le rapport

$$\frac{\mathrm{Card}\{n \in A \ / \ n \leqslant x\}}{\mathrm{Card}\{n \text{ premier } / \ n \leqslant x\}}$$

a une limite quand $x \to +\infty$, et cette limite s'appelle alors la densité (naturelle) $d(A)$ de A. Ça formalise juste l'idée imprécise que, si l'on tire un nombre premier « au hasard », la probabilité qu'il soit dans A existe et vaut $d(A)$.

L'autre notion importante, un peu plus délicate, est celle de groupe de Galois. Fixons f le polynôme à coefficients entiers, de degré $n \geqslant 1$, qui nous intéresse. On va de plus le supposer irréductible, pour simplifier : il ne s'écrit pas comme produit de deux polynômes g, h eux-mêmes à coefficients entiers (ou rationnels, c'est à peu près pareil). Il a en particulier n racines distinctes $\alpha_1, \ldots, \alpha_n$ dans $\mathbf{C}$. Alors pour comprendre beaucoup de propriétés de f, on est amené, depuis Galois (et même Lagrange en fait), à introduire un certain groupe fini, naturellement associé à f et qui caractérise en quelque sorte sa complexité. C'est l'ensemble des permutations de l'ensemble $\{\alpha_1, \ldots, \alpha_n\}$ qui, comme on disait à l'époque, préservent toutes les relations algébriques entre les racines. Autrement dit, ce sont les permutations σ telles que, pour tout polynôme $F(X_1, \ldots, X_n)$ à coefficients entiers tel que $F(\alpha_1, \ldots, \alpha_n) = 0$, on ait encore $F(\sigma\alpha_1, \ldots, \sigma\alpha_n) = 0$. On obtient ainsi un sous-groupe G du groupe $\mathfrak{S}_n$ des permutations de $\{\alpha_1, \ldots, \alpha_n\}$, qui peut aussi se voir, de manière plus moderne, comme le groupe des automorphismes du plus petit sous-corps de $\mathbf{C}$ contenant les α_k. Les travaux de Galois ont montré qu'on pouvait lire sur ce groupe énormément d'informations d'ordre algébrique sur le polynôme f (comme par exemple le fait de savoir si les racines de f peuvent s'exprimer par radicaux, c'est-à-dire à l'aide des quatre opérations et des extractions de racines k-ièmes), mais l'on s'est aperçu plus tard que G avait aussi une importance cruciale dans l'étude de *l'arithmétique* de f, et c'est à peine exagérer que de dire que la théorie des nombres moderne consiste pour beaucoup à explorer et expliciter le lien entre théorie de Galois et arithmétique.

Ces deux outils en main, on peut énoncer un cas particulier du théorème de Čebotarev, qui est un exemple assez frappant de ce fameux lien.

Théorème 1 *Soit f un polynôme non constant à coefficients entiers et irréductible. L'ensemble* $\mathrm{Spl}(f)$ *des nombres premiers p tel que f soit scindé modulo p, c'est-à-dire tels que l'on puisse écrire $f(X) \equiv (X - a_1) \cdots (X - a_n) \pmod{p}$, est infini. Mieux, il a pour densité $1/\mathrm{Card}(G)$, où G est le groupe de Galois de f.*

On peut signaler quelques exemples d'applications de l'énoncé précédent qui se traitent facilement à la main. Le premier cas est celui d'un polynôme f irréductible de degré 2, par exemple de la forme $X^2 - a$ avec a un entier qui n'est pas carré dans $\mathbf{Z}$. Un tel polynôme est scindé modulo p si et seulement s'il a une racine, donc on savait déjà que $\mathrm{Spl}(f)$ était infini. Mais comme le groupe de Galois est toujours le groupe à deux éléments (c'est facile à voir), on sait maintenant en plus que a est carré modulo la moitié des nombres premiers, et non carré modulo l'autre moitié. En particulier, en prenant $a = -1$, on obtient qu'un nombre premier sur deux est de la forme $4k + 1$. Le second cas qu'il est facile de traiter est celui de Φ_n, à condition de réussir à calculer son groupe de Galois. Il n'est pas très dur de montrer que les permutations des racines qui sont dans le groupe de Galois sont exactement celles de la forme $\sigma_k : \zeta \mapsto \zeta^k$, avec k premier à n, donc ce groupe est de cardinal $\varphi(n)$. On en déduit qu'un nombre premier sur $\varphi(n)$ est de la forme $nk + 1$.

À titre indicatif, et pour me donner l'occasion de compléter éventuellement ce petit texte plus tard, voici quand même le véritable énoncé du théorème, dans un langage que je n'expliciterai pas pour cette fois. Disons seulement que le Frobenius de f en p est un élément du groupe de Galois (défini seulement à conjugaison près) qui caractérise en particulier la façon dont f se décompose en facteurs irréductibles modulo p. Par exemple, le Frobenius est égal à l'élément neutre si et seulement si f est scindé modulo p.

Théorème 2 (Čebotarev, 1922) *Soit f un polynôme non constant à coefficients entiers et irréductible, G son groupe de Galois, et $C \subset G$ une partie stable par conjugaison. Alors l'ensemble des nombres premiers p en lesquels le Frobenius de f est dans C est de densité* $\mathrm{Card}(C)/\mathrm{Card}(G)$.

Sur ce genre de questions, et dans un style beaucoup plus clair que le mien, vous pouvez consulter l'article très joli de B. Wyman, "What is a reciprocity law ?", *American Mathematical Monthly* **79**, 1972.