UN TEST ÉLÉMENTAIRE DE PRIMALITÉ

Maurice MIGNOTTE

Le test présenté ici n'est probablement pas nouveau, bien que je ne l'aie pas trouvé dans la littérature. L'originalité de cette note est le caractère très élémentaire de sa démonstration. Contrairement aux tests usuels qui reposent sur la loi de réciprocité quadratique ou sur l'existence d'un élément primitif modulo un nombre premier, je n'utilise ici que le théorème de FERMAT, le fait que $\mathbf{Z}/p\,\mathbf{Z}$ est un corps lorsque p est un nombre premier et le théorème chinois.

Dans toute la suite n est un nombre impair ≥ 3, et on cherche à savoir si n est premier ou non. On considère les propriétés suivantes :

$$F(n) : (a,n) = 1 \Rightarrow a^{n-1} \equiv 1(\text{mod n}),$$
$$E(n) : (a,n) = 1 \Rightarrow a^{(n-1)/2} \equiv \pm 1(\text{mod n}),$$

où la notation $(a,n) = 1$ signifie que a et n sont premiers entre eux.

Le critère annoncé est le suivant.

THÉORÈME .— Soit n un entier impair, $n \geq 3$. Alors, on a l'équivalence

$$n \text{ premier} \Leftrightarrow E(n)\mathbf{et}(\exists a, a^{(n-1)/2} \equiv -1(\text{mod } n)).$$

Démontrons d'abord le résultat auxilliaire suivant.

LEMME.— Un entier n qui vérifie $F(n)$ n'est divisible par le carré d'aucun nombre premier (on dit alors que n est *quadratfrei*).

On raisonne par l'absurde. Supposons que n soit de la forme $n = p^\alpha n'$, p premier, $\alpha \geq 2$ et $(p,n') = 1$. Alors l'entier

$$x = 1 + p^{\alpha-1}$$

est d'ordre p modulo p^α, ce qui signifie que l'on a

$$x^p \equiv 1(\text{mod } p^\alpha) \text{ et } (x^k \equiv 1 \text{ mod } p^\alpha \Rightarrow p \text{ divise } k),$$

(exercice facile). D'après le théorème chinois, il existe un entier a qui vérifie

$$a \equiv x(\text{mod } p^\alpha) \text{ et } a \equiv 1(\text{mod } n').$$

Alors a est un élément d'ordre p modulo n et, comme p est premier avec $n-1$, on a

$$a^{n-1} \neq 1 (\text{mod } n).$$

D'où la conclusion.

Démonstration du théorème.

$\Longrightarrow$:

Supposons que n soit un nombre premier, $n = p$. On sait que p vérifie le théorème de FERMAT, donc pour tout entier a premier avec p, l'entier $y = a^{(n-1)/2}$ vérifie

$$y^2 \equiv 1 (\text{mod } p),$$

soit encore

$$(y-1)(y+1) \equiv 0 \ (\text{mod } p),$$

et comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, cette relation implique $y \equiv \pm 1 (\text{mod } p)$, donc $E(p)$ est vrai.

De plus, l'équation $X^{(p-1)/2} = 1$ possède au plus $(p-1)/2$ solutions dans le corps $\mathbb{Z}/p\ \mathbb{Z}$, il existe donc un y comme ci-dessus qui vérifie $y \equiv -1 (\text{mod } p)$. D'où la seconde assertion.

$\Longleftarrow$:

Supposons maintenant que n soit un entier impair ≥ 3 qui vérifie la condition $E(n)$ et tel qu'il existe un entier x vérifiant $x^{(n-1)/2} \equiv -1 (\text{mod } n)$.

Il est clair que la propriété $E(n)$ implique $F(n)$, donc le lemme montre que n est *quadratfrei*. Supposons que n ne soit pas premier, alors $n = pn'$ où p est un nombre premier et $n' > 1$, p premier avec n'.

On a

$$x^{(n-1)/2} \equiv -1 (\text{mod } p).$$

Le théorème chinois montre qu'il existe un entier a tel que

$$a \equiv x (\text{mod } p) \text{ et } a \equiv 1 (\text{mod } p).$$

Il est clair que a est premier avec n mais ne vérifie pas la condition $a^{(n-1)/2} \equiv \pm 1$ modulo n. D'où la conclusion.

La partie directe du théorème est classique. On peut noter que la preuve de la réciproque n'utilise que le théorème chinois.

Remarque : Il existe des nombres qui vérifient la propriété $E(n)$ sans être premiers, les deux plus petits sont $1729 = 7 \times 13 \times 19$ et $2465 = 5 \times 17 \times 29$.