Nombre de résidus quadratiques d'un nombre entier inférieurs à sa moitié

Denise Vella-Chemla

8.8.16

On souhaiterait démontrer qu'on peut établir le caractère de primalité d'un entier n impair en comptant le nombre (qu'on note *prq*) de ses résidus quadratiques (non nuls, on le spécifie une fois pour toutes) qui sont inférieurs ou égaux à $n/2$.

Plus précisément, on induit de comptages effectués pour les nombres impairs jusqu'à 100 l'hypothèse suivante :

(H) Si le nombre prq des résidus quadratiques d'un entier n inférieurs à n/2 est supérieur à n/4, n est premier ; sinon, n est composé.

Cette hypothèse s'écrit :

$$(H)\quad \forall p,\ p \text{ impair et } p \geq 3,$$
$$\rho(p) = \#\left\{ y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kp - y = 0 \text{ avec } 0 < y \leq \frac{p-1}{2} \right\} > \frac{n}{4}$$
$$\iff$$
$$p \text{ premier}$$

On teste notre hypothèse en la programmant : on ne peut la tester très loin car l'élévation au carré dépasse vite les limites des entiers (la limite des "unsigned long int" en C++ ne permet de tester l'hypothèse que pour des entiers inférieurs à 300 000 car on utilise un programme simple). On réalise en programmant que les nombres premiers p de la forme $4k+1$ ont leur nombre de "petits résidus quadratiques" qui est égal à $p/4$ tandis que les nombres premiers p de la forme $4k+3$ ont le nombre en question strictement supérieur à $p/4$.

Fournissons quelques éléments qui pourraient être utiles dans une démonstration.

Concernant les produits de nombres de la forme $4k+1$ ou de la forme $4k+3$, le produit de deux $4k+1$ ou le produit de deux $4k+3$ sont des $4k+1$ tandis que le produit d'un $4k+1$ et d'un $4k+3$ est un $4k+3$.

En effet,

$$\begin{array}{llll} a)\ (4k+1)(4k'+1) & = 16kk' + 4k + 4k' + 1 & = 4(4kk' + k + k') + 1 & = 4k'' + 1 \\ b)\ (4k+3)(4k'+3) & = 16kk' + 12k + 12k' + 9 & = 4(4kk' + 3k + 3k' + 2) + 1 & = 4k'' + 1 \\ c)\ (4k+1)(4k'+3) & = 16kk' + 12k + 4k' + 3 & = 4(4kk' + 3k + k') + 3 & = 4k'' + 3 \end{array}$$

Du fait de ces propriétés de la multiplication des $4k+1$ et $4k+3$, Gauss avait pour habitude de noter les $4k+3$ du signe $-$ et les $4k+1$ du signe $+$.

Pour essayer de démontrer l'hypothèse (H) émise plus haut, on peut avoir à utiliser la loi de réciprocité quadratique qui énonce :

Soient deux nombres x et y.

- *si l'un au moins de ces 2 nombres est un 4k+1, alors x est un résidu quadratique de y si et seulement si y est un résidu quadratique de x ;*
- *si les 2 nombres sont des 4k+3, alors x est un résidu quadratique de y si et seulement si y n'est pas un résidu quadratique de x.*

On va utiliser la notation $x\ R\ m$ pour exprimer que x est un résidu quadratique de m et la notation $x\ \neg R\ m$ pour exprimer que x n'est pas un résidu quadratique de m.

On rappelle la définition de *x est un résidu quadratique de m* (notée $x\ R\ m$) :

$$x\ R\ m \iff \exists y \text{ tel que } x^2 \equiv y\ (mod\ m).$$

Quelques petites règles qui illustrent des utilisations potentielles de la relation *x est un résidu quadratique de m* :

- $x\ R\ m \implies x\ R\ m^n$
- $\forall x,\ x\ R\ 2$
- $\forall k,\ (4k+1)\ R\ 4$
- $\forall k,\ (4k+3)\ \neg\ R\ 4$
- $\forall k,\ (8k+1)\ R\ 2^k$
- $\forall k,\ (8k+3)\ \neg\ R\ 2^k$
- $\forall k,\ (8k+5)\ \neg\ R\ 2^k$
- $\forall k,\ (8k+7)\ \neg\ R\ 2^k$
- $\forall x, y, m,\ x\ R\ m \text{ et } y\ R\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ \neg\ R\ m \text{ et } y\ \neg\ R\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ R\ m \text{ et } y\ \neg\ R\ m \implies xy\ \neg\ R\ m$

En annexes, sont fournis les résidus quadratiques des nombres entiers impairs de 3 à 51 inférieurs à leur moitié (dits petits résidus quadratiques) ainsi que leur nombre.

Le nombre total de résidus quadratiques de 2 et de ses puissances, ou bien d'un premier p (noté $\rho(p)$) et de ses puissances sont donnés par les formules ci-dessous :

$$\begin{aligned}
\rho(2) &= 2 \\
\rho(2^n) &= \frac{3}{2} + \frac{2^n}{6} + \frac{(-1)^{n+1}}{6} \\
\rho(p) &= \frac{p+1}{2} \\
\rho(p^n) &= \frac{3}{4} + \frac{(p-1)(-1)^{n+1}}{4(p+1)} + \frac{p^{n+1}}{2(p+1)}
\end{aligned}$$

Quelle est notre localisation actuelle ?

On sait que les points de l'espace à 3 dimensions recherchés sont les points à coordonnées entières de surfaces quadriques dégénérées d'équations de la forme $x^2 - pz - y = 0$. On représente ces points par des triplets de la forme (x, z, y). Les seuls points admissibles sont ceux dont la troisième coordonnée y vérifie les inéquations $0 < y \leq p/2$.

On ne croit pas qu'il soit possible de faire un raisonnement par récurrence parce qu'un point solution pour m n'est pas obligatoirement solution pour $m+2$: il est difficile de connaître les points qui restent petits résidus, ou bien ceux qui le deviennent alors qu'ils ne l'étaient pas, ou enfin ceux qui cessent de l'être alors qu'ils l'étaient, lors du passage de m à $m+2$.

Illustrons cela sur un exemple : le triplet $(14, 6, 10)$ est solution pour le module 31 (i.e. 14 est un petit résidu quadratique de 31) car $14^2 - 6.31 - 10 = 0$ et $14 < 31/2$. On sait que si $x^2 - y - pz = 0$ alors $x^2 - (y - 2z) - (p+2)z = 0$ et le triplet $(14, 10, 6)$ pour le module 31 pourrait être transformé en le triplet $(14, -14, 10)$ (que l'on réécrit $(14, 19, 10)$ de manière à ne traiter que d'entiers strictement positifs) pour le module 33 mais alors l'inéquations $19 \leq 33/2$ n'est pas vérifiée.

On n'arrive même pas à passer d'un petit résidu quadratique en p et d'un petit résidu quadratique en q à un petit résidu quadratique en pq : de $x^2 - y - pz = 0$ et $x'^2 - y' - qz' = 0$, on tire

$$(xx')^2 - pq(-zz') - (x^2y' + x^2qz' + x'^2y - yy' - qyz' + x'^2pz - y'pz) = 0$$

dont on ne voit pas du tout à quelle condition cela permettrait d'obtenir un petit résidu quadratique de pq.

Ces idées ne semblant pas de bonnes voies, il faudrait peut-être plutôt utiliser les chaînes de causalité entraînées par la loi de réciprocité quadratique. Voyons ces chaînes de causalité à l'oeuvre dans un exemple emprunté à Cyril Banderier : on cherche à savoir si 713 est résidu quadratique (simple, pas "petit") de 1009 (il se trouve que 713 est le carré de 210 modulo 1009) ; on effectue les calculs suivants, qui utilisent le symbole de Legendre $\frac{x}{y}$, qui vaut 1 si x est un résidu quadratique de y (i.e. si $x \; R \; y$) et -1 sinon.

$$\begin{aligned}
\left(\frac{713}{1009}\right) &= \left(\frac{1009}{713}\right)(-1)^{\frac{1008\times 712}{4}} \\
&= \left(\frac{296}{713}\right)(+1) \\
&= \left(\frac{8\times 37}{713}\right) \\
&= \left(\frac{8}{713}\right)\left(\frac{37}{713}\right) \\
&= \left(\frac{2}{713}\right)\left(\frac{37}{713}\right) \\
&= (+1)\left(\frac{37}{713}\right) \\
&= \left(\frac{713-740}{37}\right) \\
&= \left(\frac{-27}{37}\right) \\
&= \left(\frac{10}{37}\right) \\
&= \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) \\
&= (-1)\left(\frac{2}{5}\right)(-1)^{\frac{4\times 36}{4}} \\
&= (-1)(-1)(+1) \\
&= 1
\end{aligned}$$

Les opérations autorisées pour passer d'une relation $\left(\frac{a}{b}\right)$ à la relation $\left(\frac{a'}{b'}\right)$ suivante sont :

- appliquer la loi de réciprocité quadratique : intervertir a et b et multiplier le nouveau caractère de résiduosité par $(-1)^{\frac{(a-1)(b-1)}{4}}$;
- traiter comme il se doit le nombre particulier 2 ;
- remplacer un $a = p^m$ (resp. un $b = p^m$) par $a = p$ (resp. $b = p$) ;
- remplacer a ou b par leurs facteurs indépendants et réappliquer la procédure récursivement sur chaque facteur ;
- remplacer a ou b par $a - b$, $a + b$ ou $a \,\%\, b$ (i.e. $a \; mod \; b$).

Annexe 1 : petits résidus quadratiques des nombres impairs de 3 à 51

Entre parenthèses est fournie la plus petite racine carrée d'un résidu quadratique du module considéré.

$3 \to 1$.

$5 \to 1$.

$7 \to 1$, 2 (3).

$9 \to 1$, 4 (2).

$11 \to 1$, 3 (5), 4 (2), 5 (4).

$13 \to 1$, 3 (4), 4 (2).

$15 \to 1$, 4 (2), 6 (6).

$17 \to 1$, 2 (6), 4 (2), 8 (5).

$19 \to 1$, 4 (2), 5 (9), 6 (5), 7 (8), 9 (3).

$21 \to 1$, 4 (2), 7 (7), 9 (3).

$23 \to 1$, 2 (5), 3 (7), 4 (2), 6 (11), 8 (10), 9 (3).

$25 \to 1$, 4 (2), 6 (9), 9 (3).

$27 \to 1$, 4 (2), 7 (13), 9 (3), 10 (8), 13 (11).

$29 \to 1$, 4 (2), 5 (11), 6 (8), 7 (6), 9 (3), 13 (10).

$31 \to 1$, 2 (8), 4 (2), 5 (6), 7 (10), 8 (15), 9 (3), 10 (14), 14 (13).

$33 \to 1$, 3 (6), 4 (13), 9 (3), 12 (12), 15 (9), 16 (4).

$35 \to 1$, 4 (2), 9 (3), 11 (9), 14 (7), 15 (15), 16 (4).

$37 \to 1$, 3 (15), 4 (2), 7 (9), 9 (3), 10 (11), 11 (14), 12 (7), 16 (4).

$39 \to 1$, 3 (9), 4 (2), 9 (3), 10 (7), 12 (18), 13 (13), 16 (4).

$41 \to 1$, 2 (17), 4 (2), 5 (13), 8 (7), 9 (3), 10 (16), 16 (4), 18 (10), 20 (15).

$43 \to 1$, 4 (2), 6 (7), 9 (3), 10 (15), 11 (21), 13 (20), 14 (10), 15 (12), 16 (4), 17 (19), 21 (8).

$45 \to 1$, 4 (2), 9 (3), 10 (10), 16 (4), 19 (8).

$47 \to 1$, 2 (7), 3 (12), 4 (2), 6 (10), 7 (17), 8 (14), 9 (3), 12 (23), 14 (22), 16 (4), 17 (8), 18 (21), 21 (16).

$49 \to 1$, 2 (10), 4 (2), 8 (20), 9 (3), 11 (16), 15 (8), 16 (4), 18 (19), 22 (13), 23 (11).

$51 \to 1$, 4 (2), 9 (3), 13 (8), 15 (24), 16 (4), 18 (18), 19 (11), 21 (15), 25 (5).

Annexe 2 : Nombre de résidus quadratiques des nombres impairs de 3 à 51 inférieurs à leur moitié

$3 \to 1$

$5 \to 1$

$7 \to 2$

$9 \to 2$

$11 \to 4$

$13 \to 3$

$15 \to 3$

$17 \to 4$

$19 \to 6$

$21 \to 4$

$23 \to 7$

$25 \to 5$

$27 \to 6$

$29 \to 7$

$31 \to 9$

$33 \to 7$

$35 \to 7$

$37 \to 9$

$39 \to 8$

$41 \to 10$

$43 \to 12$

$45 \to 6$

$47 \to 14$

$49 \to 9$

$51 \to 9$