Nombres de résidus quadratiques des nombres premiers ou composés

Denise Vella-Chemla

28.8.2016

On souhaite préciser ici le fait qu'on peut établir le caractère de primalité d'un entier n en comptant le nombre (qu'on note $R(n)$) de ses résidus quadratiques non nuls[1].

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

- *Si n est un nombre impair :*
  - *si $R(n)$ est égal à $(n-1)/2$ alors n est premier.*
  - *si $R(n)$ est inférieur à $(n-1)/2$ alors n est composé ;*
- *Si n est un nombre pair :*
  - *si $R(n)$ est égal à $n/2$ alors n est le double d'un nombre premier ;*
  - *si $R(n)$ est inférieur à $n/2$ alors n est le double d'un nombre composé.*

Cette hypothèse peut s'écrire :

$(H1)$ $\forall n,\ n \geq 3,$

$$R(n) = \#\left\{y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ avec } 0 < y\right\} < \frac{n}{2}$$

$\iff$

n est le double d'un nombre composé s'il est pair et n est composé s'il est impair

$(H2)$ $\forall n,\ n \geq 3,$

$$R(n) = \#\left\{y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ avec } 0 < y\right\} = \frac{n}{2}$$

$\iff$

n est le double d'un nombre premier s'il est pair et n est premier s'il est impair.

Pour démontrer notre hypothèse, il faudrait prouver :

1) qu'elle est vraie par élévation d'un nombre premier p à la puissance k ;

2) qu'elle est vraie par multiplication de deux puissances de nombres premiers.

On rappelle que le nombre de résidus quadratiques d'un nombre premier p est égal à $\frac{p-1}{2}$.

Essayons de comprendre l'hypothèse heuristiquement.

Le nombre de résidus quadratiques des puissances p^k d'un nombre premier p est toujours strictement inférieur à $\frac{p^k-1}{2}$ car tous les multiples de p ne peuvent être résidus quadratiques des puissances de p.

L'identité remarquable modulaire $a^2 - b^2 \equiv (a-b)(a+b)\ (mod\ n)$ a pour conséquence une grande redondance des carrés obtenables selon le module n et cela réduit le nombre des résidus quadratiques des produits, rendant ce nombre toujours inférieur à la moitié du produit considéré.

[1] On spécifie la non-nullité des résidus considérés une fois pour toutes.

Montrons ce mécanisme sur un exemple simple (en annexe, on fournira comme autre exemple la redondance des carrés dans le cas du nombre $n = 175 = 5^2.7$).

Module $n = 35$ ($R(35) = 11$ et $11 < (35-1)/2$)

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9

Les redondances de carrés pour le module 35 sont :

$$\begin{array}{lll}
6^2 \equiv 1^2 \ (mod\ 35) & \text{car } (6-1).(6+1) = & 5.7 \quad \text{et } 35 \mid 35. \\
11^2 \equiv 4^2 \ (mod\ 35) & \text{car } (11-4).(11+4) = & 7.15 = 105 \quad \text{et } 35 \mid 105. \\
12^2 \equiv 2^2 \ (mod\ 35) & \text{car } (12-2).(12+2) = & 10.14 = 140 \quad \text{et } 35 \mid 140. \\
13^2 \equiv 8^2 \ (mod\ 35) & \text{car } (13-8).(13+8) = & 5.21 = 105 \quad \text{et } 35 \mid 105. \\
16^2 \equiv 9^2 \ (mod\ 35) & \text{car } (16-9).(16+9) = & 7.25 = 175 \quad \text{et } 35 \mid 175. \\
17^2 \equiv 3^2 \ (mod\ 35) & \text{car } (17-3).(17+3) = & 14.20 = 280 \quad \text{et } 35 \mid 280.
\end{array}$$

Le nombre de résidus quadratiques de 2 et de ses puissances, ou bien d'un premier et de ses puissances sont donnés par les formules ci-dessous :

$$\begin{array}{lll}
R(2) & = 1, & \\
R(4) & = 1, & \\
R(p) & = \dfrac{p-1}{2} & \forall\ p\ premier\ > 2 \\
R(2p) & = p & \forall\ p\ premier\ > 2 \\
R(4p) & = p & \forall\ p\ premier\ > 2 \\
R(2^k) & = \left(\dfrac{3}{2} + \dfrac{2^k}{6} + \dfrac{(-1)^{k+1}}{6}\right) - 1, & \forall\ k > 2 \\
R(p^k) & = \left(\dfrac{3}{4} + \dfrac{(p-1)(-1)^{k+1}}{4(p+1)} + \dfrac{p^{k+1}}{2(p+1)}\right) - 1 & \forall\ p\ premier\ > 2, \forall\ k \geq 2 \\
R\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) & = -1 + \prod_{i=1}^{k} \left(R\left(p_i^{\alpha_i}\right) + 1\right) &
\end{array}$$

Il est à noter que dans le cas des puissances, on soustrait 1 après avoir effectué le calcul entre parenthèses pour obtenir un nombre entier.

Bibliographie

[1] Victor-Amédée Lebesgue, *Démonstrations de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques*, Journal de Mathématiques pures et appliquées (Journal de Liouville), 1842, vol.7, p.137-159.

[2] Augustin Cauchy, Théorèmes divers sur les résidus et les non-résidus quadratiques, Comptes-rendus de l'Académie des Sciences, T10, 06, 16 mars 1840.

Annexe 1 : Redondance des carrés pour le module $175 = 5^2.7$

Pour le module 175, on écrit, sous forme de couples, les nombres qui ont même carré, on ne précise pas l'identité remarquable $a^2 - b^2 = (a - b)(a + b)$ qui est telle que les factorisations des nombres $a - b$ et $a + b$ "contiennent" tous les facteurs de $175 = 5^2.7$:

$(16, 9), (20, 15), (23, 2), (25, 10), (30, 5), (32, 18), (37, 12), (39, 11), (40, 5), (41, 34), (44, 19),$
$(45, 10), (46, 4), (48, 27), (50, 15), (51, 26), (53, 3), (55, 15), (57, 43), (58, 33), (60, 10), (62, 13),$
$(64, 36), (65, 5), (66, 59), (67, 17), (69, 6), (71, 29), (72, 47), (73, 52), (74, 24), (75, 5), (76, 1),$
$(78, 22), (79, 54), (80, 10), (81, 31), (82, 68), (83, 8), (85, 15), (86, 61), (87, 38).$

De plus, 35 et 70 ont leur carré nul et on a pris comme convention de ne pas les compter comme résidus quadratiques.

$R(175) = 43$ et $43 < (175 - 1)/2$.

Annexe 2 : Nombre de résidus quadratiques non nuls des nombres de 1 à 100

1 → 0	21 → 7	41 → 20	61 → 30	81 → 30
2 → 1	22 → 11	42 → 15	62 → 31	82 → 41
3 → 1	23 → 11	43 → 21	63 → 15	83 → 41
4 → 1	24 → 5	44 → 11	64 → 11	84 → 15
5 → 2	25 → 10	45 → 11	65 → 20	85 → 26
6 → 3	26 → 13	46 → 23	66 → 23	86 → 43
7 → 3	27 → 10	47 → 23	67 → 33	87 → 29
8 → 2	28 → 7	48 → 7	68 → 17	88 → 17
9 → 3	29 → 14	49 → 21	69 → 23	89 → 44
10 → 5	30 → 11	50 → 21	70 → 23	90 → 23
11 → 5	31 → 15	51 → 17	71 → 35	91 → 27
12 → 3	32 → 6	52 → 13	72 → 11	92 → 23
13 → 6	33 → 11	53 → 26	73 → 36	93 → 31
14 → 7	34 → 17	54 → 21	74 → 37	94 → 47
15 → 5	35 → 11	55 → 17	75 → 21	95 → 29
16 → 3	36 → 7	56 → 11	76 → 19	96 → 13
17 → 8	37 → 18	57 → 19	77 → 23	97 → 48
18 → 7	38 → 19	58 → 29	78 → 27	98 → 43
19 → 9	39 → 13	59 → 29	79 → 39	99 → 23
20 → 5	40 → 8	60 → 11	80 → 11	100 → 21