Quadratic residues numbers of prime or compound integers

Denise Vella-Chemla

28.8.2016

We would want to precise here the fact that it is possible to establish if a number is prime or not by counting the number (that we note $R(n)$) of its not null quadratic residues[1].

More precisely, we induce from countings for numbers until 100 the following hypothesis :

- *If n is an odd number :*
  - *if $R(n)$ is equal to $(n-1)/2$ then n is prime.*
  - *if $R(n)$ is lesser than $(n-1)/2$ then n is compound ;*
- *If n is an even number :*
  - *if $R(n)$ is equal to $n/2$ then n is the double of a prime number ;*
  - *if $R(n)$ is lesser than $n/2$ then n is the double of a compound number.*

Our hypothesis can be written :

$$(H1) \quad \forall n,\ n \geq 3,$$
$$R(n) = \#\left\{y \text{ such that } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ with } 0 < y\right\} < \frac{n}{2}$$
$$\iff$$
$$n \text{ is the double of a compound number if it is even and } n \text{ is compound if it is odd}$$

$$(H2) \quad \forall n,\ n \geq 3,$$
$$R(n) = \#\left\{y \text{ such that } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ with } 0 < y\right\} = \frac{n}{2}$$
$$\iff$$
$$n \text{ is the double of a prime number if it is even and } n \text{ is prime if it is odd.}$$

To demonstrate our hypothesis, one should have to prove :

1) that it is true by elevating a prime number p to the power k ;

2) that it is true by multiplying powers of primes.

We recall that the number of quadratic residues of a prime number p is equal to $\dfrac{p-1}{2}$.

Let us understand the hypothesis heuristically.

The number of quadratic residues of powers p^k of a prime number p is always strictly lesser than $\dfrac{p^k-1}{2}$ because all p's multiples can't be quadratic residues of powers of p.

The modular equivalence of differences $a^2 - b^2 \equiv (a-b)(a+b)\ (mod\ n)$ has as consequence a great redundancy of squares that can be obtained modulo n and this reduces the number of quadratic residues of products of powers, rendering this number always lesser than the half of the product considered.

[1]We will omit this non nullity of quadratic residues considered.

Let us show this redundancy mechanism on a simple example (in annex, we will provide as another example squares redundancy in the case of $n = 175 = 5^2.7$).

$Modulus\ n = 35$ ($R(35) = 11$ and $11 < (35-1)/2$)

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

Squares redundancy for modulus 35 are :

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

The quadratic residues number can be obtained by the following formulas :

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

It can be noticed that in the case of powers, 1 is substracted after the calculus between parentheses has been made to obtained an integer.

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.

Annex 1 : Squares redundancy for modulus $175 = 5^2.7$

For modulus 175, we write as couples numbers that have the same square, we don't precise the difference equality $a^2 - b^2 = (a-b)(a+b)$ that is such that factorizations of numbers $a-b$ and $a+b$ "are containing" all factors of $175 = 5^2.7$:

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

Moreover, 35 and 70 have their square that is null and we took as a convention not to count null quadratic residues.

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

Annex 2 : Not null quadratic residues numbers for integers from 1 to 100

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