Number of quadratic residues of an integer smaller than its half

Denise Vella-Chemla

26.8.2016

We would like to demonstrate that it is possible to establish primality character of an odd integer n by counting the number $R_b(n)$ of its quadratic residues (not equal to zero, we specify this once for all) that are smaller than $n/2$.

More precisely, one induces from countings concerning odd integers until 100 the following hypothesis :

(H) If $R_b(n)$ the number of quadratic residues of an integer n smaller than $n/2$ is greater than $n/4$, n is prime ; otherwise, n is compound.

This hypothesis can be written :

$$(H)\quad \forall n,\ n \text{ odd and } n \geq 3,$$
$$R_b(n) = \#\left\{ y \text{ such that } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ with } 0 < y \leq \frac{n-1}{2} \right\} > \frac{n}{4}$$
$$\iff$$
$$n \text{ is prime}$$

We test our hypothesis by coding it : we can't test it very far because squaring numbers quickly exceed integers limits (in C++, "unsigned long int" only allows us to test the hypothesis for integers lesser than 300 000 because we use a very simple program). Coding, we realize that primes p of the form $4k+1$ have their number of "small quadratic residues" that is equal to $\lfloor p/4 \rfloor$ while prime numbers p of the form $4k+3$ have the number in question strictly greater than $\lfloor p/4 \rfloor$.

We are going to use notation $x\ R\ m$ to express that x is a quadratic residue of m and notation $x\ N\ m$ to express that x is not a quadratic residue of m.

We recall the definition of *x is a quadratic residue of m* (i.e. $x\ R\ m$) :

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

We have :

- $\forall x, y, m,\ x\ R\ m \text{ and } y\ R\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ N\ m \text{ and } y\ N\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ R\ m \text{ and } y\ N\ m \implies xy\ N\ m$

In annex are provided small quadratic residues of odd integers from 3 to 51 (smaller than their half) and their number.

We recall that it is possible to deduce quadratic residuosity character of a number a prime to an odd prime number p by a simple power computing (cf. section 106 of Gauss's Arithmeticae Disquisitiones) :

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\ (mod\ p)$$

We recall that -1 is a quadratic residue of all prime numbers of the form $4k+1$ and is not a quadratic residue of all prime numbers of the form $4k+3$ (cf. section 109 of Gauss's Arithmeticae Disquisitiones).

Those particularities of quadratic residuosity character of -1 to odd prime numbers have as consequence that if p is an odd prime number of the form $4k+1$ then $r\ R\ p \iff -r\ R\ p$ while if p is an odd prime number of the form $4k+3$ then $r\ R\ p \iff -r\ N\ p$.

To demonstrate our hypothesis, we should have to prove :

1) that it's true for odd prime numbers of the form $4k+1$;

2) that it's true for odd prime numbers of the form $4k+3$;

3) that it's true by elevating a prime number p to the power k ;

4) that it's true by multiplying two prime numbers p and q ;

5) that it's true by multiplying two powers of prime numbers p^m and q^n.

1) For odd prime numbers p of the form $4k+1$, the number of quadratic residues of p that are smaller than or equal to $p/2$ is trivially equal to $\dfrac{p-1}{4}$ because in that case, r and $-r$ are systematically or both quadratic residues of p either both non-quadratic residues of p and because only one of them in each couple is smaller than or equal to $p/2$.

2) For odd prime numbers p of the form $4k+3$, Dirichlet demonstrated that there are more small quadratic residues of p than small non-quadratic residues of p using infinitesimal analysis[1] :

$$\sum_{n=1}^{n=\frac{p-1}{2}} \left(\frac{n}{p}\right) > 0.$$

In the following, *small* adjective signifies *smaller than or equal to* $p/2$ and *big* signifies *strictly greater than* $p/2$.

In [1], one can find the following invariant relations ; let us call :

- $\sum R$ the quadratic residues sum of p, an odd prime number,
- $\sum N$ its non-quadratic residues sum,
- $\sum R_b$ its "small" quadratic residues sum,
- $\sum N_b$ its "small" non-quadratic residues sum,
- $\sum R_h$ its "big" quadratic residues sum,
- $\sum N_h$ its "big" non-quadratic residues sum,
- R_b its small quadratic residues number ;
- N_b its non-quadratic residues number.

We have, if $p \equiv 7\ (mod\ 8)$:

$$\begin{cases} \sum R_b = \sum N_b. \\ \dfrac{\sum N - \sum R}{p} = R_b - N_b. \end{cases}$$

We have, if $p \equiv 3\ (mod\ 8)$:

$$\begin{cases} \sum R - \sum N = \sum R_b - \sum N_b. \\ \dfrac{3(\sum N - \sum R)}{p} = R_b - N_b. \end{cases}$$

[1] We were not able to find this Dirichlet result, possible references are *Applications de l'analyse infinitésimale à la théorie des nombres*, Journal de Crelle, 1839, vol. 19, p.324-369 or vol. 21, p.1-12 or p.134-155.

Concerning odd prime numbers of the form $p = 8k + 7$, we realize from our countings, even if we are not able to prove it, that small quadratic residues sum, that is equal, according to a result of Victor-Amédée Lebesgue, to small non-quadratic residues sum, seems equal to :

$$\sum R_b = \frac{(p-1)(p+1)}{16}.$$

There is surely a lot of functions f that are such that $f(7) = 3, f(23) = 33, f(31) = 60, f(47) = 138, f(71) = 315, f(79) = 390, f(103) = 663$ and $f(9967) = 6208818$ but $f(p) = \frac{(p-1)(p+1)}{16}$ seems relevant in this context.

So we have two sets, small quadratic residues set and small non-quadratic residues set, that share the same sum of elements, equal to $\frac{(p-1)(p+1)}{16}$, and from which we know that they don't share the same number of elements. We also know that the number 4 always belongs to the set of small quadratic residues. Those facts have perhaps as consequence that the number of small quadratic residues is always greater than the number of small non-quadratic residues.

To illustrate the idea of number superiority of small quadratic residues, let us show the modular multiplication table according to 7 modulus on 2 tables, one in which numbers are put in classical integer order and the other in which quadratic residues are enumerated before non-quadratic residues.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

	1	2	4	3	5	6
1	1	2	4	3	5	6
2	2	4	1	6	3	5
4	4	1	2	5	6	3
3	3	6	5	2	1	4
5	5	3	6	1	4	2
6	6	5	3	4	2	1

On modular multiplication table according to 23 modulus, number superiority of small quadratic residues on small non-quadratic residues appears clearly in the left-top quarter of the table. Perhaps the permutations on the classical integers order, considering them as being modular squares, has as consequence the law we observed, at least until 300 000. One can notice the horizontal and vertical symmetries.

	1	2	3	4	6	8	9	12	13	16	18	5	7	10	11	14	15	17	19	20	21	22
1	1	2	3	4	6	8	9	12	13	16	18	5	7	10	11	14	15	17	19	20	21	22
2	2	4	6	8	12	16	18	1	3	9	13	10	14	20	22	5	7	11	15	17	19	21
3	3	6	9	12	18	1	4	13	16	2	8	15	21	7	10	19	22	5	11	14	17	20
4	4	8	12	16	1	9	13	2	6	18	3	20	5	17	21	10	14	22	7	11	15	19
6	6	12	18	1	13	2	8	3	9	4	16	7	19	14	20	15	21	10	22	5	11	17
8	8	16	1	9	2	18	3	4	12	13	6	17	10	11	19	20	5	21	14	22	7	15
9	9	18	4	13	8	3	12	16	2	6	1	22	17	21	7	11	20	15	10	19	5	14
12	12	1	13	2	3	4	16	6	18	8	9	14	15	5	17	7	19	20	21	10	22	11
13	13	3	16	6	9	12	2	18	8	1	4	19	22	15	5	21	11	14	17	7	20	10
16	16	9	2	18	4	13	6	8	1	3	12	11	20	22	15	17	10	19	5	21	14	7
18	18	13	8	3	16	6	1	9	4	12	2	21	11	19	14	22	17	7	20	15	10	5
5	5	10	15	20	7	17	22	14	19	11	21	2	12	4	9	1	6	16	3	8	13	18
7	7	14	21	5	19	10	17	15	22	20	11	12	3	1	8	6	13	4	18	2	9	16
10	10	20	7	17	14	11	21	5	15	22	19	4	1	8	18	2	12	9	6	16	3	13
11	11	22	10	21	20	19	7	17	5	15	14	9	8	18	6	16	4	3	2	13	1	12
14	14	5	19	10	15	20	11	7	21	17	22	1	6	2	16	12	3	8	13	4	18	9
15	15	7	22	14	21	5	20	19	11	10	17	6	13	12	4	3	18	2	9	1	16	8
17	17	11	5	22	10	21	15	20	14	19	7	16	4	9	3	8	2	13	1	18	12	6
19	19	15	11	7	22	14	10	21	17	5	20	3	18	6	2	13	9	1	16	12	8	4
20	20	17	14	11	5	22	19	10	7	21	15	8	2	16	13	4	1	18	12	9	6	3
21	21	19	17	15	11	7	5	22	20	14	10	13	9	3	1	18	16	12	8	6	4	2
22	22	21	20	19	17	15	14	11	10	7	5	18	16	13	12	9	8	6	4	3	2	1

Let us study now the case enumerated (3) above in the aim of understanding how our hypothesis works, that is to say let us study why the number of small quadratic residues of integers n that are powers of odd prime numbers ($n = p^m$ with p an odd prime) is smaller than $n/4$.

To compute the number of small quadratic residues of p^k an odd prime number p's power, we induce formulas by analyzing first values computed by program for prime number 3 first, because it seems to have a specific behavior different from the one of other odd prime numbers, then for odd prime numbers of the form $4k+1$ powers and finally, for odd prime numbers of the form $4k+3$ powers.

From values

$$\begin{aligned} R_b(9) &= 2, \\ R_b(27) &= 6, \\ R_b(81) &= 16, \\ R_b(243) &= 47, \\ R_b(729) &= 138, \\ R_b(2187) &= 412, \\ R_b(6561) &= 1232, \\ R_b(19683) &= 3693, \end{aligned}$$

one can induce the following formula for small quadratic residues number of 3's powers.

$$R_b(3^k) = \left\lceil \frac{3^{k-1}}{2} \right\rceil + R_b(3^{k-2}).$$

From values

$$\begin{aligned} R_b(25) &= 5, \\ R_b(125) &= 26, \\ R_b(625) &= 130, \\ R_b(3125) &= 651, \\ R_b(15625) &= 3255, \end{aligned}$$

for 5's powers, and then from values

$$\begin{aligned} R_b(169) &= 39, \\ R_b(2197) &= 510, \\ R_b(28561) &= 6630, \end{aligned}$$

for 13's powers, we find the following formula for the number of small quadratic residues of powers of p for p of the form $4k+1$.

$$R_b(p^k) = kp^{k-1} + R_b(p^{k-2}).$$

Something that is amazing here is that this formula for $4k+1$ primes is also applicable to prime number 3 even if we have to consider it not as a $4k+3$ prime, what we do habitually, but rather as a $4k+1$ prime with k equal to $\frac{1}{2}$.

From values

$$\begin{aligned} R_b(7) &= 2, \\ R_b(49) &= 11, \\ R_b(343) &= 76, \\ R_b(2401) &= 526, \\ R_b(16807) &= 3678, \end{aligned}$$

for 7's powers, and then from values

$$\begin{aligned} R_b(11) &= 4, \\ R_b(121) &= 29, \\ R_b(1331) &= 308, \\ R_b(14641) &= 3358, \end{aligned}$$

for 11's powers, one can induce that the number of small quadratic residues of p powers, for p of the form $4k+3$ (except for the number 3), is close to p times the number of small quadratic residues of the power of p just before :

$$R_b(p^k) \approx pR_b(p^{k-1}).$$

It seems more sound, from a sort of symmetry principle, to interest oneself in big non-quadratic residues number (i.e. strictly greater than $\frac{n-1}{2}$), that we note $N_h(n)$. Indeed, values of $N_h(7^k)$ or of $N_h(11^k)$ are :

$$\begin{array}{ll} N_h(7) & = 2, \\ N_h(49 = 7^2) & = 14, \\ N_h(343 = 7^3) & = 97, \\ N_h(2401 = 7^4) & = 676, \end{array}$$

$$\begin{array}{ll} N_h(11) & = 4, \\ N_h(121 = 11^2) & = 34, \\ N_h(1331 = 11^3) & = 363. \end{array}$$

The approximation $N_h(p^k) \approx pN_h(p^{k-1})$ seems of better quality than the preceding one.

Concerning powers products (point (5) enumerated above), $N_h(n)$ following values,

$$\begin{array}{ll} N_h(3.7) & = 7, \\ N_h(3^2.7) & = 25, \\ N_h(3.7^2) & = 52, \\ N_h(3^2.7^2) & = 178, \end{array}$$

$$\begin{array}{ll} N_h(5.7) & = 13, \\ N_h(5^2.7) & = 68, \\ N_h(5.7^2) & = 91, \\ N_h(5^2.7^2) & = 494, \end{array}$$

$$\begin{array}{ll} N_h(13.17) & = 79, \\ N_h(13^2.17) & = 1081, \\ N_h(13.17^2) & = 1399. \end{array}$$

one can induce an approximation order for $N_h(n)$ $(p < q)$:

$$N_h(p^m.q^n) \approx p.N_h(p^{m-1}.q^n)$$

Concerning small quadratic residues numbers for which values are following,

$$\begin{array}{ll} R_b(3.7) & = 4, \\ R_b(3^2.7) & = 9, \\ R_b(3.7^2) & = 22, \\ R_b(3^2.7^2) & = 45, \end{array}$$

$$\begin{array}{ll} R_b(5.7) & = 7, \\ R_b(5^2.7) & = 24, \\ R_b(5.7^2) & = 34, \\ R_b(5^2.7^2) & = 123, \end{array}$$

$$\begin{array}{ll} R_b(13.17) & = 31, \\ R_b(13^2.17) & = 355, \\ R_b(13.17^2) & = 479. \end{array}$$

even if we can't provide rules for their progression, one can see that studied values always verify :

$$R_b(p^m.q^n) < p.R_b(p^{m-1}.q^n).$$

The number of small quadratic residues for powers of prime numbers of the form $p = 4k + 3$ (except for the case $p = 3$) is always strictly lesser than $\frac{p^k - 1}{4}$ because all p multiples can't be quadratic residues of p powers, and that decreases considerably the number of small quadratic residues.

We can now show explicitly the mechanism that is operating for products, this mechanism having as consequence a very great redundancy of squares obtained, and this reduced considerably their number, making it always lesser than $n/4$.

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

Combinatorics operating, even if it explains clearly the decreasing of the number of small quadratic residues number for compound numbers, is too complicated to allow us to find a formula that would give directly the number of small quadratic residues by a function of n.

Module $n = 35$ ($R_b(35) = 7$ and $7 < 35/4$)

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 redundancies for 35 modulus are :

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

It remains to study simple primes product case of the form $p.q$ with p and q primes (point (4) of the plan above). Study suggests that the number of small quadratic residues $R_b(pq)$ is close to $\frac{R_b(p^2) + R_b(q^2)}{4}$, always smaller than $\frac{pq}{4}$. The elimination mechanism of redundant squares because of difference of two squares identity is again applicable, decreasing the number of small quadratic residues.

Finally, if our objective is to formally demonstrate our hypothesis rather using group theory, perhaps the following fact should be considered for counting quadratic residues of different primes powers products : there is a sort of products "triangle" that are responding themselves ; a $8k+3$ and a $8k'+7$ product is a $8k''+5$, one of a $8k+3$ and of a $8k'+5$ is a $8k''+7$ and one of a $8k+5$ and of a $8k'+7$ is a $8k''+3$.

Conclusion

We realize, once redundancy squares mechanism has been studied and understood, that a simpler criterion that allows us to distinguish odd prime numbers from odd compound ones is that the former have their number of quadratic residues that is equal to $\frac{p-1}{2}$ while the latter have this number that is strictly lesser than $\frac{p-1}{2}$.

Bibliography

[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.

Annex 1 : Redundancy of squares for modulus $175 = 5^2.7$

For modulus 175, one writes, in couples form, numbers that have the same square, we don't provide the explanation $a^2 - b^2 = (a-b)(a+b)$ showing that $a-b$ and $a+b$ factorizations "cover" all prime 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 equal to 0 modulo 175 and we chose not to count them as small quadratic residues.

Annex 2 : Small quadratic residues of odd numbers from 3 to 51 and their number

Between parentheses is provided the smallest squareroot of each small quadratic residue of the considered modulus.

3 → 1.	→ 1
5 → 1.	→ 1
7 → 1, 2 (3).	→ 2
9 → 1, 4 (2).	→ 2
11 → 1, 3 (5), 4 (2), 5 (4).	→ 4
13 → 1, 3 (4), 4 (2).	→ 3
15 → 1, 4 (2), 6 (6).	→ 3
17 → 1, 2 (6), 4 (2), 8 (5).	→ 4
19 → 1, 4 (2), 5 (9), 6 (5), 7 (8), 9 (3).	→ 6
21 → 1, 4 (2), 7 (7), 9 (3).	→ 4
23 → 1, 2 (5), 3 (7), 4 (2), 6 (11), 8 (10), 9 (3).	→ 7
25 → 1, 4 (2), 6 (9), 9 (3), 11 (6).	→ 5
27 → 1, 4 (2), 7 (13), 9 (3), 10 (8), 13 (11).	→ 6
29 → 1, 4 (2), 5 (11), 6 (8), 7 (6), 9 (3), 13 (10).	→ 7
31 → 1, 2 (8), 4 (2), 5 (6), 7 (10), 8 (15), 9 (3), 10 (14), 14 (13).	→ 9
33 → 1, 3 (6), 4 (13), 9 (3), 12 (12), 15 (9), 16 (4).	→ 7
35 → 1, 4 (2), 9 (3), 11 (9), 14 (7), 15 (15), 16 (4).	→ 7
37 → 1, 3 (15), 4 (2), 7 (9), 9 (3), 10 (11), 11 (14), 12 (7), 16 (4).	→ 9
39 → 1, 3 (9), 4 (2), 9 (3), 10 (7), 12 (18), 13 (13), 16 (4).	→ 8
41 → 1, 2 (17), 4 (2), 5 (13), 8 (7), 9 (3), 10 (16), 16 (4), 18 (10), 20 (15).	→ 10
43 → 1, 4 (2), 6 (7), 9 (3), 10 (15), 11 (21), 13 (20), 14 (10), 15 (12), 16 (4), 17 (19), 21 (8).	→ 12
45 → 1, 4 (2), 9 (3), 10 (10), 16 (4), 19 (8).	→ 6
47 → 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).	→ 14
49 → 1, 2 (10), 4 (2), 8 (20), 9 (3), 11 (16), 15 (8), 16 (4), 18 (19), 22 (13), 23 (11).	→ 11
51 → 1, 4 (2), 9 (3), 13 (8), 15 (24), 16 (4), 18 (18), 19 (11), 21 (15), 25 (5).	→ 10