The Quadratic Character of 2

RAFAEL JAKIMCZUK
Universidad Nacional de Luján
Buenos Aires, Argentina
jakimczu@mail.unlu.edu.ar

There are many proofs of the quadratic character of 2. The text by Ireland and Rosen contains a non-elementary proof [**1**, p. 69] and an elementary proof using Gauss's Lemma [**1**, p. 53], and there are also combinatorial proofs [**3, 2**]. Euler, in an early paper, proved that 2 is a quadratic residue of primes of the form $8k + 1$ [**1**, p. 70], assuming the existence of a primitive root modulo p. Later, Gauss was the first to give a rigorous proof that primitive roots exist. In this short note we give a complete, elementary proof of the quadratic character of 2 assuming the existence of a primitive root mod p.

THEOREM. *The number* 2 *is a quadratic residue of primes of the form* $p = 8k + 1$ *and* $p = 8k + 7$. *The number* 2 *is not a quadratic residue of primes of the form* $p = 8k + 3$ *and* $p = 8k + 5$.

Proof. Let p be an odd prime and let g be a primitive root modulo p. The set $\{1, 2, \ldots, p-1\}$ can be written in the form $\{g^1 = g, g^2, g^3, \ldots, g^{p-1} = 1\}$.

Note that $g^{\frac{p-1}{2}} = p - 1$ since $(g^{\frac{p-1}{2}})^2 = 1$. Also, g^n is a quadratic residue if and only if n is even.

Consider the following system of $\frac{p-1}{2} - 1$ congruences, all mod p.

$$\begin{aligned} g^1(1 + g^{(p-1)-1}) &= (1 + g^1) \\ g^2(1 + g^{(p-1)-2}) &= (1 + g^2) \\ g^3(1 + g^{(p-1)-3}) &= (1 + g^3) \\ &\vdots \\ g^{\frac{p-1}{2}-1}(1 + g^{\frac{p-1}{2}+1}) &= (1 + g^{\frac{p-1}{2}-1}) \end{aligned}$$

Consider the sums $(1 + g^k)$ that that appear either on the right side, or as the second factor on the left side. Every residue appears exactly once in one of these positions except for the values $0 = (1 + g^{\frac{p-1}{2}})$, $1 = (1 + 0)$, and $2 = (1 + g^{p-1})$.

In each congruence, if the first factor is a quadratic residue then the second factor and the product have the same character—that is, both are quadratic residues or neither is a quadratic residue. On the other hand, if the first factor is a quadratic nonresidue then the second factor and the product have opposite character. Consequently each congruence contains an odd number of quadratic residues.

The rest of the proof is a simple counting argument. We may think of the system of congruences as a table with three columns. In the first column are the powers of g from g^1 to $g^{(p-1)/2-1}$, and in the second and third columns are the various sums $(1 + g^k)$.

Suppose $p = 8k + 1$.

(a) The table contains an odd number of congruences, each containing an odd number of quadratic residues, so the number of quadratic residues in the table is odd. The

number of quadratic residues in the first column is $2k - 1$ (count the even powers of g), which is also odd. So the number of quadratic residues in the second and third columns must be even. But those columns contain every number in Z/pZ exactly once, except for 0, 1, and 2. So the number of quadratic residues in Z/pZ, other than 0, 1, and 2, is even.

(b) But the number of quadratic residues in Z/pZ, other than 0 and 1, is $(p-1)/2 - 1 = 4k - 1$, which is odd.

(c) Since (a) and (b) differ, 2 must be a quadratic residue.

Suppose $p = 8k + 3$.

(a) The table contains an even number of congruences, each containing an odd number of quadratic residues, so the number of quadratic residues in the table is even. The number of quadratic residues in the first column is $2k$, which is also even. So the number of quadratic residues in the second and third columns must be even. But those columns contain every number in Z/pZ exactly once, except for 0, 1, and 2. So the number of quadratic residues in Z/pZ, other than 0, 1, and 2, is even.

(b) But the number of quadratic residues in Z/pZ, other than 0 and 1, is $4k$, which is even.

(c) Since (a) and (b) coincide, 2 cannot be a quadratic residue.

The other cases ($p = 8k + 5$ and $p = 8k + 7$) work the same way. The theorem is thus proved. ■

Acknowledgment The author is very grateful to Universidad Nacional de Luján.

Dedication In memory of my sister Fedra Marina Jakimczuk, 1970–2010.

REFERENCES

1. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, New York, 1998.
2. R. Jakimczuk, The quadratic equation in F_p and the quadratic reciprocity law, *International Journal of Contemporary Mathematical Sciences* **4** (2009) 419–431.
3. K. S. Williams, The quadratic character of 2 (mod p), *Mathematics Magazine* **49** (1976) 89–90. doi:10.2307/2689440

Summary The number 2 is a quadratic residue mod p if $p = 8k + 1$ or $p = 8k + 7$, but not if $p = 8k + 3$ or $p = 8k + 5$. This is proved by a simple counting argument, assuming the existence of a primitive root mod p.