

# The American Mathematical Monthly

|  |      |
|--|------|
| The Captain William Lowell Rouse Hurlbut Memorial            | 475  |
| Journal of the American Mathematical Society                 |      |
| Journal of Number Theory                                     | 488  |
| Journal of Algebra   | 504  |
| Journal of Combinatorial Theory                              | 517  |
| Journal of the London Mathematical Society                   | 526  |
| Journal of the American Statistical Association              | 534  |
| Journal of the Institute of Mathematics and its Applications | 537  |
| Journal of the American Chemical Society                     | 544  |
| Journal of the American Physical Society                     | 552  |
| Journal of the American Medical Association                  | 560  |
| Journal of the American Veterinary Association               | 568  |
| Journal of the American Dental Association                   | 576  |
| Journal of the American Pharmacological Association          | 584  |
| Journal of the American Psychological Association            | 592  |
| Journal of the American Musicological Society                | 600  |
| Journal of the American Historical Association               | 608  |
| Journal of the American Library Association                  | 616  |
| Journal of the American Library Association                  | 624  |
| Journal of the American Library Association                  | 632  |
| Journal of the American Library Association                  | 640  |
| Journal of the American Library Association                  | 648  |
| Journal of the American Library Association                  | 656  |
| Journal of the American Library Association                  | 664  |
| Journal of the American Library Association                  | 672  |
| Journal of the American Library Association                  | 680  |
| Journal of the American Library Association                  | 688  |
| Journal of the American Library Association                  | 696  |
| Journal of the American Library Association                  | 704  |
| Journal of the American Library Association                  | 712  |
| Journal of the American Library Association                  | 720  |
| Journal of the American Library Association                  | 728  |
| Journal of the American Library Association                  | 736  |
| Journal of the American Library Association                  | 744  |
| Journal of the American Library Association                  | 752  |
| Journal of the American Library Association                  | 760  |
| Journal of the American Library Association                  | 768  |
| Journal of the American Library Association                  | 776  |
| Journal of the American Library Association                  | 784  |
| Journal of the American Library Association                  | 792  |
| Journal of the American Library Association                  | 800  |
| Journal of the American Library Association                  | 808  |
| Journal of the American Library Association                  | 816  |
| Journal of the American Library Association                  | 824  |
| Journal of the American Library Association                  | 832  |
| Journal of the American Library Association                  | 840  |
| Journal of the American Library Association                  | 848  |
| Journal of the American Library Association                  | 856  |
| Journal of the American Library Association                  | 864  |
| Journal of the American Library Association                  | 872  |
| Journal of the American Library Association                  | 880  |
| Journal of the American Library Association                  | 888  |
| Journal of the American Library Association                  | 896  |
| Journal of the American Library Association                  | 904  |
| Journal of the American Library Association                  | 912  |
| Journal of the American Library Association                  | 920  |
| Journal of the American Library Association                  | 928  |
| Journal of the American Library Association                  | 936  |
| Journal of the American Library Association                  | 944  |
| Journal of the American Library Association                  | 952  |
| Journal of the American Library Association                  | 960  |
| Journal of the American Library Association                  | 968  |
| Journal of the American Library Association                  | 976  |
| Journal of the American Library Association                  | 984  |
| Journal of the American Library Association                  | 992  |
| Journal of the American Library Association                  | 1000 |


ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: <https://www.tandfonline.com/loi/uamm20>

## A Counting Proof for When 2 Is a Quadratic Residue


Karthik Chandrasekhar, Richard Ehrenborg & Frits Beukers



To cite this article: Karthik Chandrasekhar, Richard Ehrenborg & Frits Beukers (2020) A Counting Proof for When 2 Is a Quadratic Residue, *The American Mathematical Monthly*, 127:8, 750-751, DOI: [10.1080/00029890.2020.1790925](https://doi.org/10.1080/00029890.2020.1790925)

To link to this article: <https://doi.org/10.1080/00029890.2020.1790925>

 Published online: 21 Sep 2020.

 Submit your article to this journal 

 Article views: 303

 View related articles 

 View Crossmark data 

---

# A Counting Proof for When 2 Is a Quadratic Residue

---

Karthik Chandrasekhar, Richard Ehrenborg, and Frits Beukers

---

**Abstract.** Using the group consisting of the eight Möbius transformations  $x, -x, 1/x, -1/x, (x-1)/(x+1), (x+1)/(1-x), (x+1)/(x-1),$  and  $(1-x)/(x+1),$  we present an enumerative proof of the classical result for when the element 2 is a quadratic residue in the finite field  $F_q.$

Recall that a nonzero element  $x$  in a field  $F$  is a *quadratic residue* if it is a square, that is, we can write  $x = y^2$  where  $y \in F.$

Assume that  $q$  is an odd prime power and let  $F_q$  be the finite field of  $q$  elements. The classical result that  $-1$  is a quadratic residue in  $F_q$  if and only if  $q \equiv 1 \pmod{4}$  can be proved by partitioning the nonzero elements of the field into orbits of the form  $\{x, -x, -1/x, 1/x\}.$  Note that one orbit is  $\{1, -1\}.$  If  $\alpha^2 = -1$  has a solution, then  $\{\alpha, -\alpha\}$  is also an orbit. The remaining orbits all have cardinality 4. Thus by counting the nonzero elements of the field modulo 4, we obtain that  $q \equiv 1 \pmod{4},$  implying that  $q - 1 \equiv 0 \equiv |\{1, -1\}| + |\{\alpha, -\alpha\}| \pmod{4}$  and hence that the orbit  $\{\alpha, -\alpha\}$  exists, that is,  $-1$  is a quadratic residue. Similarly,  $q \equiv 3 \pmod{4}$  implies that there is no such orbit and hence  $-1$  is not a quadratic residue. See [1, Theorem 2.2.7].

We present a similar argument for when the element 2 is a quadratic residue. We use a larger set of rational functions and we have four different types of orbits.

**Theorem 1.** *Let  $q$  be an odd prime power. Then the element 2 is a quadratic residue in the finite field  $F_q$  if and only if  $q \equiv \pm 1 \pmod{8}.$*

*Proof.* Consider the eight rational functions  $x, -x, 1/x, -1/x, (x-1)/(x+1), (x+1)/(1-x), (x+1)/(x-1),$  and  $(1-x)/(x+1).$  Note that they form a group  $G$  under composition. These rational functions are Möbius transformations and act naturally on the field  $F_q$  with the point at infinity adjoined, that is, on  $F_q \cup \{\infty\}.$  The orbits of this action are as follows. First there is the orbit  $\{0, \pm 1, \infty\}.$  In fact, the group permutes these elements as the vertices of a square, showing that the group is isomorphic to the symmetric group of a square. Assuming that 2 is a quadratic residue in the field  $F_q,$  we have the orbit  $B = \{\pm 1 \pm \sqrt{2}\}$  of size 4. Next, assuming that  $-1$  is a quadratic residue, we have the orbit  $C = \{\pm i\}$  of size 2. Finally, the remaining orbits all have size 8.

We now have four cases. In each case, it is enough to count the  $q - 3$  elements in  $F_q - \{0, \pm 1\}$  modulo 8, hence only keeping track if the orbits  $B$  and  $C$  occur.

- If  $-1$  and 2 are both quadratic residues, then both  $B$  and  $C$  occur, yielding  $q - 3 \equiv 4 + 2 \pmod{8},$  that is,  $q \equiv 1 \pmod{8}.$
- If  $-1$  and 2 are both not quadratic residues, then all orbits have size 8, yielding  $q - 3 \equiv 0 \pmod{8},$  that is,  $q \equiv 3 \pmod{8}.$

---

[doi.org/10.1080/00029890.2020.1790925](https://doi.org/10.1080/00029890.2020.1790925)

MSC: Primary 11A07

- If  $-1$  is a quadratic residue and  $2$  is not, then only  $C$  occurs, yielding  $q - 3 \equiv 2 \pmod{8}$ , that is,  $q \equiv 5 \pmod{8}$ .
- Finally, if  $2$  is a quadratic residue and  $-1$  is not, then only  $B$  occurs, yielding  $q - 3 \equiv 4 \pmod{8}$ , that is,  $q \equiv 7 \pmod{8}$ . ■

A similar proof can be obtained by using the order 6 group  $H = \{x, 1 - x, 1/(1 - x), x/(x - 1), (x - 1)/x, 1/x\}$ . When  $q \equiv 3 \pmod{4}$ , the result follows by counting the number of quadratic residues in orbits of  $H$ . Similarly, when  $q \equiv 1 \pmod{4}$ , the result follows by counting the number of quadratic nonresidues.

**ACKNOWLEDGMENTS.** The authors thank David Leep for suggestions that improved the exposition of an earlier version of this note. This work was partially supported by a grant from the Simons Foundation (#429370 to Richard Ehrenborg).

#### REFERENCE

---

- [1] Davidoff, G., Sarnak, P., Valette, A. (2003). *Elementary Number Theory, Group Theory, and Ramanujan Graphs*. Cambridge, UK: Cambridge Univ. Press.

*Department of Mathematics, University of Kentucky, Lexington, KY, USA*  
[ak.c@uky.edu](mailto:ak.c@uky.edu)

*Department of Mathematics, University of Kentucky, Lexington, KY, USA*  
[richard.ehrenborg@uky.edu](mailto:richard.ehrenborg@uky.edu)

*Department of Mathematics, University of Utrecht, 3508 TA Utrecht, The Netherlands*  
[f.beukers@uu.nl](mailto:f.beukers@uu.nl)