5.4: Introduction to Quadratic Residues and Nonresidues

The question that we need to answer in this section is the following. If \((p)\) is an odd prime and \((a)\) is an integer relatively prime to \((p)\). Is \((a)\) a perfect square modulo \((p)\).

Let \((m)\) be a positive integer. An integer \((a)\) is a quadratic residue of \((m)\) if \(((a,m)=1)\) and the congruence \((x^2\equiv a \pmod m)\) is solvable. If the congruence \((x^2\equiv a \pmod m)\) has no solution, then \((a)\) is a quadratic nonresidue of \((m)\).

Notice that \((1^2=6^2\equiv 1\pmod 7), (3^2=4^2\equiv 2\pmod 7)\) and \((2^2=5^2\equiv 4\pmod 7)\). Thus \((1,2,4)\) are quadratic residues modulo 7 while \((3,5,6)\) are quadratic nonresidues modulo 7.

Let \((p\neq 2)\) be a prime number and \((a)\) is an integer such that \((p\nmid a)\). Then either \((a)\) is a quadratic nonresidue modulo \((p)\) or \([x^2\equiv a\pmod p]\) has exactly two incongruent solutions modulo \((p)\).

If \([x^2\equiv a\pmod p]\) has a solution, say \((x=x^\prime)\), then \((-x^\prime)\) is a solution as well. Notice that \((-x^\prime \not\equiv x^\prime \pmod p)\) because then \((p|2x^\prime)\) and hence \((p\nmid x^\prime)\).

We now show that there are no more than two incongruent solutions. Assume that \((x=x^\prime)\) and \((x=x^\prime)\) are both solutions of \([x^2\equiv a\pmod p]\). Then we have \([(x^\prime)^2-(x^\prime)^2=(x^\prime+x^\prime)(x^\prime-x^\prime)\equiv 0\pmod p].\) Hence \([x^\prime\equiv x^\prime\pmod p]\) \lor \([x^\prime\equiv -x^\prime\pmod p]\).

The following theorem determines the number of integers that are quadratic residues modulo an odd prime.

If \((p\neq 2)\) is a prime, then there are exactly \(((p-1)/2)\) quadratic residues modulo \((p)\) and \(((p-1)/2)\) quadratic nonresidues modulo \((p)\) in the set of integers \((1,2,...,p-1)\).
To find all the quadratic residues of \(p\) among all the integers \(1,2,...,p-1\), we determine the least positive residue modulo \(p\) of \(1^2,2^2,...,(p-1)^2\). Considering the \((p-1)\) congruences and because each congruence has either no solution or two incongruent solutions, there must be exactly \((p-1)/2\) quadratic residues of \(p\) among \(1,2,...,p-1\). Thus the remaining are \(((p-1)/2)\) quadratic nonresidues of \(p\).

**Exercises**

1. Find all the quadratic residues of 3.

2. Find all the quadratic residues of 13.

3. Find all the quadratic residues of 18.

4. Show that if \(p\) is prime and \(p \geq 7\), then there are always two consecutive quadratic residues of \(p\). Hint: Show that at least one of \(2,5\) or 10 is a quadratic residue of \(p\).

5. Show that if \(p\) is prime and \(p \geq 7\), then there are always two quadratic residues of \(p\) that differ by 3.

**Contributors**

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s [Open Textbook Challenge](https://www.saylor.org/) for public release under a Creative Commons Attribution (CC BY) license.