N7: Quadratic

Amy Creel
MATH 361B

April 5, 2019

Number of Quadratic Residues:

When I was looking at the number of quadratic residues in $\mathbb{Z}_p$ for prime numbers up to $p = 53$, I noticed that the number of quadratic residues is equal to $(p + 1)/2$. For example, $(23 + 1)/2 = 12$, and 12 is the number of quadratic residues in Z_{23}. The only numbers for which this doesn't work are 1 and 2, because the number of quadratic residues in $\mathbb{Z}_1$ is 1 and the number of quadratic residues in $\mathbb{Z}_2$ is 2.

If -1 is a Quadratic Residue:

It looks as though if $p - 1$ is divisible by 4, then $\mathbb{Z}_p$ will have -1 as a quadratic residue (with the exception of 1 and 2, which do not follow this pattern but both have -1 as a quadratic residue). For example, prime numbers up to 53 with -1 as a quadratic residue (excluding 1 and 2) are: $5, 13, 17, 29, 37, 41$ and 53. Then the "-1" in these scenarios are: $4, 12, 16, 28, 36, 40$ and 52. So, the pattern seems to be that if -1 in $\mathbb{Z}_p$ is divisible by four, then $\mathbb{Z}_p$ will have -1 as a quadratic residue.