Melbourne High School
Maths Extension Group 2023
Term 3 Week 4 Handout Solutions

Quadratic Residues

1. Enumerating the squares modulo 17, the squares are $1, 4, 9, 16, 8, 2, 15, 13$. Since $16 \equiv -1$ the congruence is solvable.

2. (a) If a and b are both nonresidues, then $(a|p) = -1$ and $(b|p) = -1$. But ab is a residue, so $(ab|p) = 1 = (a|p)(b|p)$. If both a and b are residues, then $(a|p) = 1$, $(b|p) = 1$, and $(ab|p) = 1$; and again $(ab|p) = (a|p)(b|p)$. For the last case, we may assume with loss of generality that $(a|p) = -1$ and $(b|p) = 1$; then $(ab|p) = -1 = (a|p)(b|p)$ and the proof is complete.

   (b) If $(a|p) = 1$ and $a \equiv x^2 \pmod p$, then it follows that $b \equiv x^2$ also if $a \equiv b$. Thus $(a|p) = (b|p)$. If $(a|p) = -1$, suppose that there exists some x such that $b \equiv x^2 \pmod p$. But since $b \equiv a$ that would mean $a \equiv x^2$, which is a contradiction. Hence no such x exists, and so $(a|p) = -1 = (b|p)$.

3. From a property of the Legendre symbol we have

$$\left(\frac{-1}{p}\right) = \left(\frac{(p-1)!}{p}\right).$$

The number $(p-1)!$ consists of the product of all the numbers from 1 to $p-1$. We know that amongst those numbers exactly $(p-1)/2$ of them are quadratic residues and exactly $(p-1)/2$ of them are quadratic nonresidues. The product of the quadratic residues will give a quadratic residue, so whether $(p-1)!$ is a residue or nonresidue depends only on whether the product of the $(p-1)/2$ nonresidues gives a residue or nonresidue. Recall that the product of two nonresidues gives a residue; hence if the number of nonresidues is even, the resulting product will be a residue, and if the number of nonresidues is odd, then the resulting product will be a nonresidue. When is $(p-1)/2$ even and when is it odd? If it is to be even, then $p-1$ must be a multiple of 4, and hence $p \equiv 1 \pmod 4$. If it is to be odd, then $p-1$ must an odd multiple of 2, so that that $(p-1)/2$ is not further divisible by 2. Hence $p - 1 = 2(2k+1)$ from which it follows that $p = 4k+3$, or $p \equiv 3 \pmod 4$. Hence

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Observe that since $(-1|p)$ depends on whether the number of nonresidues $(p-1)/2$ is even or odd, the result can be also be written more succinctly as

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$