1 Review of Number Theory

Definition 1 We say \(a\) is congruent to \(b\) modulo \(n\), denoted as \(a \equiv b \mod n\), if \(n|a - b\) i.e. there exists \(k \in \mathbb{Z}\) such that \(n \cdot k = a - b\).

Example 1 Consider the equation \(x^2 \equiv 3 \mod 7\). Can we find a solution to this?
Well we can try to plug in all values from \(\{1, \ldots, 6\}\) to see all possible values for \(x^2\) (we will be ignoring 0 in this worksheet).

\[
\begin{align*}
1^2 &\equiv 1 \mod 7, \quad 2^2 \equiv 4 \mod 7, \quad 3^2 \equiv 2 \mod 7, \quad 4^2 \equiv 2 \mod 7, \quad 5^2 \equiv 4 \mod 7, \quad 6^2 \equiv 1 \mod 7
\end{align*}
\]

We can see that the squares are \(\{1, 4, 2\}\) \(\mod 7\). However, this is a bit of a tedious process to find solutions to the above equation. We will explore different methods to find solutions to equations of the form \(x^2 \equiv a \mod p\) for \(\gcd(a, p) = 1\).

Definition 2 Suppose \(a \in \mathbb{N}\), \(p\) prime such that \(\gcd(a, p) = 1\), and consider the equation \(x^2 \equiv a \mod p\). If there is a solution \(x_0\) such that \(x_0^2 \equiv a \mod p\), we say that \(a\) is a **Quadratic Residue** \(\mod p\). If there is no solution, we say that \(a\) is a **(Quadratic) Non-residue** \(\mod p\). (Note: 0 is neither a quadratic residue nor non-residue). We write QR and NR for shorthand.

Problem 1 Consider the case where \(p = 2\). Why is this case not very interesting? What are the only choices we have for \(a\) such that \(\gcd(a, p) = 1\)? Is such a a QR or NR? After this problem, we will only consider the odd primes.

Problem 2 Notice in Example 1 that we get a pattern: \(1, 4, 2, 2, 4, 1\). This is symmetric. Prove that for all \(x \in \{1, \ldots, p - 1\}\) that \(x^2 \equiv (p - x)^2 \mod p\).
**Problem 3** Let $p$ be an odd prime. Show that there are exactly $(p - 1)/2$ QR’s and NR’s.

1. We know that the QR’s are the numbers $1^2, 2^2, \ldots, (p - 1)^2$. Use problem 2 to show that we can reduce this list to $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ and still have all of the QR’s.

2. Check that all of the numbers in the list $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are different mod $p$.

3. Conclude there are $(p - 1)/2$ QR’s AND NR’s.
Example 2 Before we can prove some theorems about QR’s, we need some properties of a certain list of numbers $a, 2a, \ldots, (p-1)a$ where $p$ is prime and $p \nmid a$. If we write out this list for $p = 7$ and $a = 4$ and reduce mod $p$, we get

$$4, 1, 5, 2, 6, 3$$

Notice we get all of the numbers $1, \ldots, p - 1$.

**Problem 4** Let $p$ be a prime number, and $a \in \mathbb{N}$ such that $p \nmid a$. Then the list $a, 2a, 3a, \ldots, (p-1)a \mod p$ has the same numbers as the list $1, 2, 3, \ldots, p-1 \mod p$ up to rearrangement.

1. Show that none of $a, 2a, 3a, \ldots, (p-1)a$ are divisible by $p$. (Use the prime divisibility property $p \mid ab$ implies ...?)

2. Suppose two numbers in the list were congruent mod $p$, $ja \equiv ka \mod p$. Use the prime divisibility property again to show that $j = k$, and conclude the list has all distinct elements mod $p$. 


Problem 5  Show that the product of two QR’s is a QR i.e. if $a_1, a_2$ are QR’s, then $a_1a_2$ is a QR.

Problem 6  Show that the product of a QR and an NR is an NR i.e. if $a_1$ is a QR and $a_2$ is an NR then $a_1a_2$ is an NR.

1. Suppose that $a_1a_2$ is a QR. By definition, $a_1a_2 = b_2^2$ and $a_1 = b_1^2$ for some $b_1, b_2$. What is $gcd(b_1, p)$? Can we find an inverse for $b_1 \mod p$?

2. Show that $a_2$ is a QR and derive a contradiction.
Problem 7 Show that the product of two NR’s is a QR i.e. if \( a_1, a_2 \) are NR’s then \( a_1a_2 \) is a QR. (Hint: consider the list \( a_1, 2a_1, \ldots, (p-1)a_1 \). Use problems 3, 4, 6)
Problem 8  We have the following formulas from problems 4-6:

\[ QR \times QR = QR \quad QR \times NR = NR \quad NR \times NR = QR \]

Can you think of any integers \( QR, NR \in \mathbb{Z} \) where \( QR \neq NR \) that satisfy these relations?

Definition 3  Suppose \( p \) is an odd prime, and \( a \in \mathbb{N} \) such that \( p \nmid a \). Then define the Legendre Symbol of \( a \) modulo \( p \) as

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a QR mod } p \\
-1 & \text{if } a \text{ is an NR mod } p
\end{cases}
\]

Problem 9  Suppose \( p \) is an odd prime. Using problems 4-6, show the Legendre symbol satisfies the multiplicative property

\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right)
\]
Problem 10 Calculate \( \left( \frac{75}{97} \right) \)

Problem 11 When is \( \left( \frac{-1}{p} \right) = 1 \)? Calculate this value for some small odd primes. Conjecture when \( \left( \frac{-1}{p} \right) = 1 \) and when \( \left( \frac{-1}{p} \right) = -1 \). We will prove it next time.