Worksheet 1: Quadratic Residues

An element \( r \) in a ring \( R \) is called an \( n \)th root of unity if \( r^n = r \cdot r \cdot \cdots r = 1 \).

More generally an element is called a root of unity if it is an \( n \)th root of unity for some \( n \).

**Problem 1.1:**
In the following rings determine which elements are \( n \)th roots of unity for \( n = 1, 2, 4 \).

1. \( F_3 \)
2. \( F_5 \)
3. \( F_7 \)
4. \( \mathbb{Q} \)

**Solution 1.1:**
Let $p$ be an odd prime number.

**Problem 1.2:**

1. Show that the product of all the different nonzero elements in $\mathbb{F}_p$ is equal to $p - 1$.
2. Show that every nonzero element in $\mathbb{F}_p$ is a $(p - 1)$th root of unity.

**Solution 1.2:**
We say that $m$ is a quadratic residue modulo $p$ if there exists some integer $x$, such that
\[ x^2 \equiv m \pmod{p}. \]

We define the Legendre symbol as follows
\[
\left( \frac{m}{p} \right) = \begin{cases} 
0 & \text{if } p \text{ divides } m \\
1 & \text{if } m \text{ is a quadratic residue modulo } p \\
-1 & \text{if } m \text{ is not a quadratic residue modulo } p 
\end{cases}
\]

Problem 1.3:
Compute the following Legendre symbols:
1. \( \left( \frac{2}{3} \right) \)
2. \( \left( \frac{4}{7} \right) \)
3. \( \left( \frac{3}{5} \right) \)
4. \( \left( \frac{8}{11} \right) \)

Solution 1.3:
For the following problems you may use without proof the following fact: For any prime number $p$, there exists a number $\alpha$, such that, any nonzero number in $\mathbb{F}_p$ can be written as $\alpha^n$ for some $n$.

**Problem 1.4:**
Show that $\left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

**Solution 1.4:**
Problem 1.5:
Show that the Legendre symbols satisfies the following property:

\[ \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \]

Solution 1.5:
Law of quadratic reciprocity

Let $q$ and $p$ be odd prime numbers, then:

$$\left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4} \left( \frac{p}{q} \right)$$

Problem 1.6:

Use the law of quadratic reciprocity and the multiplicative property to compute the following:

(1) $\left( \frac{15}{67} \right)$
(2) $\left( \frac{17}{113} \right)$
(3) $\left( \frac{9411}{9283} \right)$

Solution 1.6:
The Legendre symbol allows us to determine when an element is a quadratic residue modulo $p$, i.e. when an element in $\mathbb{F}_p$ has a square root, without having to compute the squares of all possible elements. Now we will focus on how to find a square root if it exists.

Problem 1.7:

Let $p$ be a prime number, with $p \equiv 3 \pmod{4}$.

Show that if $\left( \frac{a}{p} \right) = 1$, then $a^{\frac{p+1}{4}}$ is a square root of $a$ (in $\mathbb{F}_p$).

Solution 1.7:
Let $p$ be an odd prime number. It may be written as $p = 2^r s + 1$, where $s$ is an odd number and $r$ is a positive integer.

**Problem 1.8:**
Show that if $\left(\frac{a}{p}\right) = 1$, then there exists a $2^r$th root of unity $\mu$, such that: $\mu \frac{a^{s+1}}{2}$ is a square root of $a$ (in $\mathbb{F}_p$).

**Solution 1.8:**
Let $p$ be an odd prime number. It may be written as $p = 2^r s + 1$, where $s$ is an odd number and $r$ is a positive integer.

**Problem 1.9:**
Show that if $\left( \frac{b}{p} \right) = -1$, then any $2^r$th root of unity is a power of $b^s$ (in $\mathbb{F}_p$).

**Solution 1.9:**
Problem 1.10:
Find if the following elements have square roots, and if they do compute them.
(1) 15 in $\mathbb{F}_{37}$
(2) 35 in $\mathbb{F}_{73}$
(3) 186 in $\mathbb{F}_{401}$
(4) 168921 in $\mathbb{F}_{35227}$

Solution 1.10:
Problem 1.11:
Using the previous problems give a list of steps to determine if an element of $\mathbb{F}_p$ has a square root (in $\mathbb{F}_p$) and how to find them if they exist.

Solution 1.11:
Problem 1.12:
Find for which primes $p$ the following polynomials have solutions in $\mathbb{F}_p$:
1. $x^2 + 7$
2. $x^2 + 3x - 2$
3. $x^2 + 6x + 15$
4. $x^4 + 2x^3 + 17x^2 + 30x + 30$

Solution 1.12:
Problem 1.13:
Show that in a field there are at most $n$ different $n$th roots of unity.
Is this true for rings that are not fields?
Hint: Notice that a root of unity is a solution to the equation $x^n = 1$.

Solution 1.13: