QUADRATIC RESIDUES

DEFINITION: We say that an element $x \in \mathbb{Z}_n$ is a **square** or a **quadratic residue** if there is some $y \in \mathbb{Z}_n$ such that $y^2 = x$, and in this case, we call y a **square root** of x.

(1) Let n be an odd positive integer. Suppose that $[a]$ is a unit in $\mathbb{Z}_n$. Show that[1] the solutions x to the equation $[a]x^2 + [b]x + [c] = [0]$ in $\mathbb{Z}_n$ are exactly the elements of the form

$$x = \frac{-[b] + u}{[2a]} \quad \text{such that } u \text{ is a square root of } [b^2 - 4ac].$$

Since we assumed $[a]$ is a unit, we can rewrite as $x^2 + \frac{[b]}{[a]}x + \frac{[c]}{[a]} = [0]$. Since n is odd, $[2]$ is a unit too, so we can complete the square:

$$\begin{aligned}
[0] &= x^2 + \frac{[b]}{[a]}x + \frac{[c]}{[a]} \\
&= x^2 + [2]\frac{[b]}{[2a]}x + \left(\frac{[b]}{[2a]}\right)^2 - \left(\frac{[b]}{[2a]}\right)^2 + \frac{[c]}{[a]} \\
&= \left(x + \frac{[b]}{[2a]}\right)^2 + \frac{[4ac - b^2]}{[4a^2]},
\end{aligned}$$

so

$$\left(\frac{[2a]x + [b]}{[2a]}\right)^2 = \frac{[b^2 - 4ac]}{[4a^2]}.$$

Thus, x is a solution if and only if $[2a]x + [b]$ is a square root of $[b^2 - 4ac]$. Rearranging slightly gives the form above.

(2) Let p be an odd prime and $x \in \mathbb{Z}_p^\times$. Show that if x is a quadratic residue, then x has exactly two square roots $y \neq y'$, and for these roots, $y' = -y$.

If $y^2 - x = 0$ has a solution, it has at most two since this is a polynomial of degree two over a field. If y is a solution, then $y' = -y$ is too.

(3) Let p be a prime number and g be a primitive root of $\mathbb{Z}_p$. Show that $[n] \in \mathbb{Z}_p^\times$ is a quadratic residue if and only if the index of $[n]$ with respect to g is even.

Write $[n] = g^k$, so the index is k. If $k = 2\ell$ is even, then $[n] = g^k = g^{2\ell} = (g^\ell)^2$, so $[n]$ is a quadratic residue. Conversely, if $[n] = [m]^2$, write $[m] = g^\ell$, so $[n] = [m]^2 = g^{2\ell}$. If $2\ell < p - 1$, this is the index of $[n]$; otherwise, we subtract a multiple of $p - 1$ to get back to the index, and since $p - 1$ is even, the result is even, so the index is even.

[1] Hint: Complete the square!