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 $[n] = [m]^2 = g^{2\ell}$, which is even. (Note that even and odd are well-defined in $\mathbb{Z}_{p-1}$ for p odd, since any two representatives differ by a multiple of two.)

[1] Hint: Complete the square!

DEFINITION: Let p be an odd prime. For $r \in \mathbb{Z}$ not a multiple of p we define the **Legendre symbol** of r with respect to p as

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if } [r] \text{ is a square in } \mathbb{Z}_p, \\ -1 & \text{if } [r] \text{ is a not square in } \mathbb{Z}_p. \end{cases}$$

THEOREM (EULER'S CRITERION): For p an odd prime and $r \in \mathbb{Z}$ not a multiple of p, we have

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

THEOREM (QUADRATIC RECIPROCITY PART -1): If p is odd, then

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

PROPOSITION: Let p be an odd prime and a, b integers not divisible by p. Then

(1) $a \equiv b \pmod{p}$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(3) $\left(\frac{a^2}{p}\right) = 1$.

(4) (a) Without using the Proposition above, explain why $\left(\frac{4}{p}\right) = 1$ for p an odd prime. Now explain why part (3) of the Proposition above is true in general.

(b) Use the Proposition above to explain the following: If a, b are not squares modulo p, then ab is a square modulo p.

(c) Use[2] the Proposition and Corollary above to determine how many solutions x to

$$[3]x^2 + [12]x - [2] = [0]$$

there are in $\mathbb{Z}_{43}$.

(a) $[4] = [2]^2$; $[a^2] = [a]^2$.

(b) We have $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, so $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^2 = 1$.

(c) Using the quadratic formula, we need to determine whether $[12^2 - 4 \cdot 3 \cdot -2] = [168]$ is a square in $\mathbb{Z}_{43}$. By the hint, we have $168 = 4 \cdot 42$, so

$$\left(\frac{168}{43}\right) = \left(\frac{4}{43}\right)\left(\frac{42}{43}\right) = 1\left(\frac{-1}{43}\right) = 1 \cdot -1 = -1.$$

[2] You might find it convenient to write $168 = 4 \cdot 42$.

We conclude that there are no solutions.

(5) Use problem #3 to prove Euler's criterion.

Let $g = [a]$ be a primitive root and write $[r] = g^k$ for some k.

If $[r]$ is a residue, then $k = 2\ell$ is even, and $r^{(p-1)/2} \equiv a^{2\ell(p-1)/2} \equiv a^{\ell(p-1)} \equiv 1 \pmod{p}$ by FLT.

If $[r]$ is not a residue, then $k = 2\ell + 1$ is odd, and $r^{(p-1)/2} \equiv a^{(2\ell+1)(p-1)/2} \equiv a^{\ell(p-1)+(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}$ by FLT. We know that $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ again by FLT, so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. But, by definition of primitive root, $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, so $a^{(p-1)/2} \equiv -1 \pmod{p}$.

(6) Prove the proposition above.

We already did part (3). Part (1) is clear since the value of $\left(\frac{a}{p}\right)$ only depends on the congruence class of a modulo p. For (2), take a primitive root $g = [r]$ and write $a \equiv r^k, b \equiv r^\ell$. Then, by Euler's criterion,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv r^{k\frac{p-1}{2}} r^{\ell\frac{p-1}{2}} \equiv r^{(k+\ell)\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

(7) Use Euler's criterion to prove QR part -1 above.

If $p \equiv 1 \pmod{4}$, write $p = 4k+1$; then $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1$, so -1 is a residue by Euler's criterion. If $p \equiv 3 \pmod{4}$, write $p = 4k+3$; then $(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1$, so -1 is not a residue by Euler's criterion.

(8) When n is not a prime...
   (a) Does the conclusion of #4(b) hold if n is replaced by a general positive integer n instead of a prime p?
   (b) Suppose that $n = pq$ for primes $p \neq q$. Show that a is a quadratic residue modulo n if and only if a is a quadratic residue modulo p and a quadratic residue modulo q.