Quadratic Residues

Reading

- Section 11.1

Practice Problems

11.1 1-10, 14, 15, 16, 26
11.1 (Challenge, Optional) 30, 31
11.2 1-6, 10

Notes

Quadratic residues

Quadratic residues are just a fancy way of talking about whether an element is a square or not:

> We say that $0 \neq \bar{a} \in \mathbb{Z}_n$ is a **quadratic residue** modulo n if there is a b such that $\bar{b}^2 = \bar{a}$.
>
> A non-zero number that is not a quadratic residue is called a **quadratic nonresidue** modulo n.
>
> 0 is considered neither.

Our main goal in this section is to develop ways to determine when a number is a quadratic residue. We start with a simple observation:

> If $p > 2$ is a prime and $\bar{a} \in \mathbb{Z}_p$ is a quadratic residue, then there are *exactly two* elements in $\mathbb{Z}_p$ such that $\bar{x}^2 = \bar{a}$.
>
> As a consequence, exactly $\frac{p-1}{2}$ quadratic residues modulo p, therefore exactly $\frac{p-1}{2}$ quadratic nonresidues.

To prove this:

- Suppose that $b^2 = a$. Then we also have that $(-b)^2 = a$.
- We must show that $b \neq -b$.
  - If it were the case, then we would have $2b = 0$.
  - Since 2 is invertible when $p > 2$, we would get $b = 0$, which is of course a contradiction.
- Since the polynomial $x^2 - a$ has at most two roots,

Legendre Symbol

The Legendre Symbol is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } \bar{a} \text{ quadratic residue modulo } p \\ -1 & \text{if } \bar{a} \text{ quadratic nonresidue modulo } p \\ 0 & \text{if } \bar{a} = 0 \end{cases}$$

Note that this only depends on $a \bmod p$, and not on a itself.

It essentially captures the information as to whether a is a quadratic residue or not.

Examples:

$\left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = -1$ because the only squares modulo 7 are 1, 2, 4.

Similarly $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$.

One really important property of the Legendre Symbol is that it is multiplicative:

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

This will follow from the following results:

1. If a or b is divisible by p, then so is their product.
2. If a and b are quadratic residues, then so is their product.
3. If a is a quadratic residue and b is a quadratic nonresidue, then their product is a quadratic nonresidue.
4. If a and b are quadratic nonresidues, then ab is a quadratic residue.

Let us prove these:

- Part 1 is straightforward, as is part 2.
- For part 3:
  - Note that a^{-1} is also a quadratic residue.
  - If ab was a quadratic residue, then $b = a^{-1}ab$ is a quadratic residue by part 2. Which is a contradiction.
- For par 4:
  - Consider the operation: multiplication by a. We know it must be 1-1.
  - By part 3 we know it takes the $\frac{p-1}{2}$ quadratic residues to the $\frac{p-1}{2}$ quadratic nonresidues.
  - Therefore it must take the remaining $\frac{p-1}{2}$ quadratic nonresidues to the $\frac{p-1}{2}$ quadratic residues.
  - So ab must be a quadratic nonresidue.

Euler's identity

Euler's identity offers us another way to determine the quadratic residues.

> Let $p > 2$ and $0 \neq \bar{a} \in \mathbb{Z}_p$.
>
> 1. If $\bar{a}$ is a quadratic residue, then $\bar{a}^{\frac{p-1}{2}} = \bar{1}$.
> 2. If $\bar{a}$ is a quadratic nonresidue, then $\bar{a}^{\frac{p-1}{2}} = -\bar{1}$.
> 3. (Euler's identity) We have:
>
> $$\left(\frac{a}{p}\right) = \bar{a}^{\frac{p-1}{2}} \bmod p$$

Let us prove these:

1. Suppose $\bar{a}$ is a quadratic residue.
   - So $\bar{a} = \bar{b}^2$.
   - Then $\bar{a}^{\frac{p-1}{2}} = b^{p-1} = 1$ by Fermat's theorem.
2. This is the challenging part. Suppose $\bar{a}$ is a quadratic nonresidue.
   - For each number c in $1, 2, \ldots, p-1$ modulo p, we have that $d = c^{-1}a \neq c$, as otherwise we would have $c^2 = a$ and a would have been a quadratic residue.
   - So the numbers from 1 to $p-1$ can be grouped up in pairs, each pair multiplying to $\bar{a}$.
   - Therefore the product of all those numbers equals $\bar{a}^{\frac{p-1}{2}}$.
   - By Wilson's theorem the product also equals $-\bar{1}$.
3. This more or less follows from the two previous cases, and the trivial case where $a = 0 \bmod p$.

Use this method to determine the quadratic residues modulo 7.

There are two important consequences of Euler's identity. The first is that, as we saw previously in a more complicated way, the Legendre symbol behaves multiplicatively. This follows directly as it relates to a (fixed) power of a, and raising to a power behaves multiplicatively on the base.

The other is the determination of when -1 is a quadratic residue.

The quadratic character of -1

Euler's identity gives us a way to find when -1 is a quadratic residue. We have:

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

> So:

- If $p = 1 \bmod 4$, i.e. $\frac{p-1}{2}$ is even, then -1 is a quadratic residue modulo p.
- If $p = 3 \bmod 4$, i.e. $\frac{p-1}{2}$ is odd, then -1 is a quadratic nonresidue modulo p.