Quadratic Residues (Week 3 - Monday)

We studied the equation $ax \equiv b \bmod m$ and solved it when $\gcd(a,m) = 1$. I left it as an exercise to investigate what happens when $\gcd(a,m) \neq 1$ [Hint: There are no solutions to $ax \equiv 1 \bmod m$]. Thus, we have completely understood the equation $ax \equiv b \bmod m$. Then we took it one step further and found simultaneous solutions to a set of linear equations. The next natural step is to consider quadratic congruences.

Example 1 Find the solutions of the congruence $15x^2 + 19x \equiv 5 \bmod 11$.

A We need to find x such that $15x^2 + 19x - 5 \equiv 4x^2 + 8x - 5 \equiv (2x-1)(2x+5) \equiv 0 \mod 11$. Since 11 is prime, this happens iff $2x - 1 \equiv 0 \mod 11$ or $2x + 5 \equiv 0 \bmod 11$. Now you can finish this problem by using the techniques described in the previous lectures. In particular, $2^{-1} \equiv 6 \mod 11$ and we have $x \equiv 6 \mod 11$ or $x \equiv -30 \equiv 3 \bmod 11$. ■

So let's start by investigating the simplest such congruence: $x^2 \equiv a \bmod m$.

Definition 2 Let p a prime number. Then the integer a is said to be a **quadratic residue** of p if the congruence $x^2 \equiv a \mod p$ has a solution. More generally, if m is any positive integer, we say that a is a quadratic residue of m if $\gcd(a,m) = 1$ and the congruence $x^2 \equiv a \mod m$ has a solution. If a is not a quadratic residue it's said to be a **quadratic non-residue**.

Example 3

- 2 is a quadratic residue of 7 because $3^2 \equiv 2 \bmod 7$
- 5 is a quadratic non-residue of 7: This is seen by checking $a^2 \bmod 7$ for all the 7 possible values of $a \bmod 7$.

Example 4 Which integers are quadratic residues of 11?

A Since any integer is of the form $n = 11q + r$ with $0 \leq r < 11$, we have $n^2 \equiv r^2 \mod 11$. Thus, we just need to square 11 integers. Squaring we obtain, $r \in \{0, 1, 4, 9, 5, 3\}$ i.e. n is a quadratic residue iff $n = 11q + r$ for r in that set.

Lemma 5 Show that if p is an odd prime and a is an integer not divisible by p, then the congruence $x^2 \equiv a \bmod p$ has either no solutions or exactly two incongruent solutions modulo p.

Proof Assume that there is at least one solution, call it y. Let z be another solution to $x^2 \equiv a \bmod p$. Then, $y^2 \equiv z^2 \mod p$ and thus $(y-z)(y+z) \equiv 0 \mod p$. Since p is prime this implies $y - z \equiv 0 \bmod p$ or $y + z \equiv 0 \bmod p$. Thus, $\{y \bmod p, -y \bmod p\}$ are two solutions to the congruence. If $y \equiv -y \mod p$, then $2y \equiv 0 \bmod p$. Since p is odd this implies that $p|y$ and thus $p|a$; this is a contradiction. ■

Corollary 6 Show that if p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p among the integers $1, 2, \ldots, p-1$.

Proof We are asking for the cardinality of the set $S = \{1^2 \bmod p, 2^2 \bmod p, 3^2 \bmod p, \ldots, (p-1)^2 \bmod p\}$. Lemma 5 implies that $x^2 \equiv y \bmod p$ has at most two solutions. Thus, there are at least $\frac{p-1}{2}$ distinct elements in S. If there were less than $\frac{p-1}{2}$ distinct elements, then there would be three distinct solutions to $x^2 \equiv y \bmod p$ for some y.

Conversely, since $a \bmod p$ and $(p-a) \equiv -a \bmod p$ both square to the same element S, there are at most $\frac{p-1}{2}$ distinct elements in S. Thus $|S| = \frac{p-1}{2}$. ■

Example 7 Find all solutions of the congruence $x^2 \equiv 29 \bmod 35$. [Hint: Find the solutions of this congruence modulo 5 and modulo 7, and then use the Chinese remainder theorem.]

A First of all Lemma 5 implies that this equation has at most four solutions. Indeed, a solution y to $x^2 \equiv 29 \bmod 35$ would also be a solution to $x^2 \equiv 29 \bmod 5$ and $x^2 \equiv 29 \bmod 7$. Each of these have at most 2 solutions, in particular, $y \bmod 35$ will have at most four possibilities. We will now find four solutions, by solving these congruences mod5 and mod7 and combining them using the Chinese remainder theorem.

First we explicitly establish Bezout's identity, namely $5 \cdot 3 - 7 \cdot 2 = 1$. Then, $x^2 \equiv 29 \equiv 4 \bmod 5$ has the solutions $x \equiv \pm 2 \bmod 5$ and $x^2 \equiv 29 \equiv 1 \bmod 7$ has the solutions $x \equiv \pm 1 \mod 7$. Thus, we obtain the four solutions $y \equiv \pm 2 \cdot (-2 \cdot 7) \pm 1 \cdot (3 \cdot 5) \equiv \mp 28 \pm 15 \bmod 35$ i.e. $y \in \{\pm 8 \bmod 35, \pm 13 \bmod 35\}$. ■

Definition 8 If p is an odd prime and a is an integer not divisible by p, the **Legendre symbol**, denoted $\left(\frac{a}{p}\right)$, is defined to be

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{otherwise} \end{cases}.$$

If $p|a$, we define $\left(\frac{a}{p}\right) = 0$.

Example 9 $\left(\frac{3}{3}\right) = 0$, $\left(\frac{1}{3}\right) = 1$, $\left(\frac{2}{3}\right) = -1$.

Notice that if p is a prime number and a, b are integers such that $a \equiv b \bmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. We now prove a very important relation that allows us to figure out if an integer is a quadratic residue without computing it's square root! The proof of the theorem relies on two important results we have proven in previous lectures/worksheets.

Theorem 10 [**Euler's criterion**] Let p be an odd prime and a a positive integer not divisible by p, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.

Proof First assume that a is a quadratic residue. Then $\left(\frac{a}{p}\right) = 1$ and $a = x^2$ for some integer x. Then by Fermat's little theorem we have $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \bmod p$ as required.

Now assume that a was not a quadratic residue. Then consider the set $\{1, 2, 3, \ldots, p-1\}$. The trick is to notice that for every $c \in S$ we can solve $cx \equiv a \bmod p$ and obtain $c' \neq c$ (since a is **not** a quadratic residue!) such that $cc' \equiv a \bmod p$. This gives us a partition of S into pairs and we can group all these pairs together in the product $1 \cdot 2 \cdot 3 \cdots (p-1)$ to obtain,

$$\begin{aligned} (p-1)! &\equiv a^{\frac{p-1}{2}} \\ &\equiv a^{\frac{p-1}{2}} \bmod p. \end{aligned}$$

By Wilson's theorem, $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \bmod p$. ■

We can now state the law of Quadratic Reciprocity, one of the most famous theorems in mathematics. This was first proven by Gauss in 1796, and he liked it so much that he found eight different proofs in his lifetime.

Quadratic Reciprocity For any two odd primes p, q we have,

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

Example 11 Is there a solution to $x^2 \equiv 3 \bmod 79$ i.e. is 3 a quadratic residue mod79.

A Since a brute force search is very tedious, we will appeal to the law of quadratic reciprocity. This gives us, $\left(\frac{3}{79}\right)\left(\frac{79}{3}\right) = (-1)^{\frac{2}{2}\cdot\frac{78}{2}} = -1$. Since $79 \equiv 1 \bmod 3$, 79 is a quadratic residue modulo 3 i.e. $\left(\frac{79}{3}\right) = 1$. Thus, $\left(\frac{3}{79}\right) = -1 \cdot \left(\frac{79}{3}\right)^{-1} = -1$ i.e. 3 is **not** a quadratic residue modulo 79!