Chapter 11: Quadratic Residues

Greg Knapp

March 8, 2022

1 Quadratic Residues and Nonresidues

1.1 Intro

- Now that we've learned how to solve linear equations mod m, it would be great if we could also solve quadratic equations mod m.
- Big Question: Is there a quadratic formula mod m?
- Let's start with simple quadratic equations first.
- Given a and m, can we solve $x^2 \equiv a \mod m$?
- Some examples:
  - Mod 7:

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

  - Mod 6:

x	0	1	2	3	4	5
x^2	0	1	4	3	4	1

  - Mod 15:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1

- Some observations:
  - The tables are symmetric (because $x^2 \equiv (-x)^2 \mod m$)
  - Mod 7 works like we expect: 0 has one square root (itself), everything else has two square roots
  - Note that we find that 2 is a square mod 7. This is not so in the usual integers
  - Mod 6 is a little weird: 3 only has one square root
  - Mod 15 is terrible: 4 has 4 square roots. 1 has 4 square roots. 10 has 2 square roots
  - It's a veritable mess
- The plan: First study when $x^2 \equiv a \mod p$ has solutions
- See if we can build from there
- Note: this is a huge and well-studied topic in number theory. I don't have all the answers off the top of my head, but most questions about square roots mod m have answers.
- **Def:** If $m > 0$, we say that a is a quadratic residue mod m if $(a, m) = 1$ and $x^2 \equiv a \mod m$ has a solution. If $x^2 \equiv a \mod m$ has no solution, then a is a quadratic nonresidue mod m

1.2 How Many Square Roots?

- Lemma: Let p be an odd prime and $a \in \mathbb{Z}$ not a multiple of p. Then $x^2 \equiv a \mod p$ has either 0 or two incongruent solutions mod p.
- Proof:
  - Suppose $x^2 \equiv a \mod p$ doesn't have 0 solutions.
  - Then it has one, say y
  - If it has another, say z, then we have that $y^2 \equiv a \equiv z^2 \mod p$
  - Then $p \mid y^2 - z^2 = (y-z)(y+z)$
  - So $p \mid y - z$ or $p \mid y + z$
  - So $y \equiv z \mod p$ or $-y \equiv z \mod p$
  - Hence, the only two possible solutions are $\pm y$
  - Could $\pm y$ be the equivalent mod p
  - If yes, then $y - (-y) \equiv 0 \mod p$, i.e. $p \mid 2y$
  - $p \nmid 2$ since p is odd, so $p \mid y$.
  - But then $a \equiv y^2 \equiv 0 \mod p$, contradicting our assumption that a is not a multiple of p
  - Hence, $y \not\equiv -y \mod p$, so $\pm y$ are the two distinct solutions.
- Theorem: If p is an odd prime, there are exactly $(p-1)/2$ quadratic residues of p and $(p-1)/2$ quadratic nonresidues of p
- Proof:
  - Consider the function

$$\begin{aligned} \{1, 2, \ldots, p-1\} &\to \{1, 2, \ldots, p-1\} \\ x &\mapsto x^2 \mod p \end{aligned}$$

  - By the lemma, this map is two-to-one
  - So its image is half the size of the domain: i.e. $\frac{p-1}{2}$ elements that are quadratic residues
  - The rest are nonresidues: $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ of them
- **Def:** Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

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

- **Ex:** We previously found that $\left(\frac{0}{7}\right) = 0$, $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$ and $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$

1.3 How Do We Calculate the Legendre Symbol?

- Theorem (Euler's Criterion): Let p be an odd prime and let $a \in \mathbb{Z}$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

- Proof:
  - If $p \mid a$, then both sides are 0 mod p

- Otherwise, suppose $\left(\frac{a}{p}\right) = 1$
- Then there exists $x \in \mathbb{Z}$ so that $x^2 \equiv a \mod p$
- Then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p$, check
- Now suppose $\left(\frac{a}{p}\right) = -1$
- We want to think of $a^{\frac{p-1}{2}}$ in a clever way
- The idea is going to be to break it up into pairs.
- For each $1 \leqslant i \leqslant p-1$, there exists $1 \leqslant j \leqslant p-1$ satisfying $ij \equiv a \mod p$ (take $j = ai^{-1}$)
- Moreover, $j \neq i$ because there are no solutions to $x^2 \equiv a \mod p$
- But then looking at $(p-1)!$ we can decompose the product into $\frac{p-1}{2}$ pairs with $ij \equiv a$ and so we have
$$-1 \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \mod p$$
and we again, get what we want

- **Ex:** Let $p = 17$ and $a = 5$. Decide whether 5 is a quadratic residue mod 17.
  - Since $\left(\frac{5}{17}\right) \equiv 5^{\frac{17-1}{2}} \mod 17$, we compute $5^8 \mod 17$:
$$\begin{aligned} 5^2 &\equiv 25 \equiv 8 \mod 17 \\ 5^4 &\equiv 64 \equiv 13 \equiv -4 \mod 17 \\ 5^8 &\equiv (-4)^2 \equiv 16 \equiv -1 \mod 17 \end{aligned}$$
  - Hence, 5 is not a quadratic residue mod 17

- Theorem: Let p be an odd prime. Then
  1. If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
  2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
  3. $\left(\frac{a^2}{p}\right) = 1$

- Proof:
  - The first and third parts are trivial, though useful
  - The second part uses Euler's criterion and follows from writing it out...

- Corollary: The product of two squares is a square. The product of a square and a nonsquare is a nonsquare. The product of two nonsquares is a square.

1.4 When is -1 a Quadratic Residue of p?

- Note that we can rephrase this as: When is there a square root of $-1 \mod p$? Just how the square root of -1 is pretty important in other parts of math, this has important consequences in number theory.

- Theorem: If p is an odd prime, then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$

- Proof:
  - If $p \equiv 1 \mod 4$ if and only if $\frac{p-1}{2}$ is even, so $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p$

1.5 When is 2 a Quadratic Residue of p?

- When $p \equiv \pm 1 \mod 8$.
- No time for proof!

2 The Law of Quadratic Reciprocity

- **Thm:** Let p and q be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$
- Rather than trying to prove this, we're going to consider an equivalent formulation and examples.
- **Thm:** Suppose p is an odd prime and $a \in \mathbb{Z}$. If q is a prime with $p \equiv \pm q \mod 4a$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$
- Reformulated, when computing $\left(\frac{a}{p}\right)$, you can replace p by any prime congruent to it mod $4a$
- **Ex:** Decide whether 3 is a quadratic residue mod 101
  - Note that $101 \equiv 5 \mod 12$, so $\left(\frac{3}{101}\right) = \left(\frac{3}{5}\right)$. It is easy to check that 3 is not a square mod 5 and hence, not a square mod 101
- Going back to the main statement $\frac{p-1}{2}\cdot\frac{q-1}{2}$ is even when either $p \equiv 1 \mod 4$ or $q \equiv 1 \mod 4$.
- Hence $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ if and only if $q \equiv p \equiv 3 \mod 4$
- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ if and only if $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are different
- I.e. $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$
- Hence, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if and only if $p \equiv q \equiv 3 \mod 4$
- Otherwise, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- We're pretty much only going to practice using this theorem for computations:
- **Ex:** Is 13 a square mod 17?
  - Both 13 and 17 are 1 mod 4, so $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$
  - Now we reduce to $\left(\frac{4}{17}\right) = \left(\frac{2^2}{17}\right) = 1$
  - Hence, the answer is yes.
- **Ex:** Is 7 a square mod 19?
  - Both 7 and 19 are 3 mod 4, so $\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right)$
  - Reducing mod 7 gives $\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right)$
  - 5 is 1 mod 4, so $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right)$
  - Since 5 is neither $\pm 1 \mod 8$, $\left(\frac{2}{5}\right) = -1$
  - Hence, 7 is a square mod 19
- **Ex:** Is 713 a square mod 1009? (1009 is prime)
  - $713 = 23 \cdot 31$, so we can write $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\cdot\left(\frac{31}{1009}\right)$
  - Now $1009 \equiv 1 \mod 4$, so $\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right)$

– Also $\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right)$
– Factoring gives $\left(\frac{20}{23}\right) = \left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{5}{23}\right)$ and since $5 \equiv 1 \mod 4$, we get $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right)$
– By quadratic reciprocity, $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$
– Now, focus on

$$\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right)$$
$$= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

– Multiplying now gives $\left(\frac{713}{1009}\right) = 1$, so 713 is a square mod 1009.