Announcements:

- Course Evals!
- Portfolio 2: probably today, maybe tomorrow

Section 11.1: Quadratic Residues

Q: Is there a "quadratic formula" mod m?

A: complicated

Analogy: $\mathbb{R}$

1. Given $ax^2+bx+c=0$, are there solns?
   ↳ if $b^2-4ac \geq 0$, yes. Otherwise, no.
2. If so, what are they?

Examples. $x^2 \equiv a \mod m$

- $\exists$ soln. to $x^2 \equiv a \mod m$ iff a has a sq. rt. mod m.

$5 \equiv -2 \mod 7$

$(5)^2 \equiv \underbrace{(-2)^2}_{2^2} \mod 7$

$m = 7$

x	0	1	2	3	4	5	6
least. pos. res. of x^2 mod 7	0	1	4	2	2	4	1

$m = 6$

x	0	1	2	3	4	5
l.p.r. of x^2 mod 6	0	1	4	3	4	1

$m = 15$

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

x	13	14
x^2	4	1

Observations:

- mod 7 works how we expect:
  - 0 has one sq. rt.
  - everything else has 0 or 2 sq. rts.

- mod 6 does not:
  ↳ 3 has one sq. rt.

- mod 15 does not:
  ↳ 4 has 4 sq. rts.
  1 has 4 sq. rts.
  10 has 2 sq. rts.

The plan: $x^2 \equiv a \mod p$ when p is prime.

Def: If $m > 0$, we say that a is a <u>quadratic residue</u> mod m if $(a, m) = 1$ and there exists $x \in \mathbb{Z}$ s.t. $x^2 \equiv a \mod m$

If $x^2 \equiv a \mod m$ has no solns. then a is a <u>quadratic nonresidue</u>

mod m.

How many squares / square rts?

Lemma: If p is an odd prime and $a \in \mathbb{Z}$ is not a multiple of p, then $x^2 \equiv a \bmod p$ has either zero or two incongruent solns.

Pf: Suppose $x^2 \equiv a \bmod p$ doesn't have zero solns.

(Goal: show there are two solns.)

So $\exists\, y \in \mathbb{Z}$ s.t. $y^2 \equiv a \bmod p$.

Suppose also $z \in \mathbb{Z}$ has $z^2 \equiv a \bmod p$

(Goal: show $z \equiv \pm y \bmod p$)

$y^2 \equiv a \equiv z^2 \mod p$

$p \mid y^2 - z^2 = (y-z)(y+z)$

Since p is prime, $p \mid y-z$

or $p \mid y+z$

So either $y \equiv z \mod p$ or $y \equiv -z \mod p$

Next: show that $y \not\equiv -y \mod p$

Suppose $y \equiv -y \mod p$

$\rightarrow p \mid 2y$ $\rightarrow$ $p \mid 2$ $\times$ p odd

or

$\rightarrow$ $p \mid y \rightarrow p \mid y^2$

$\rightarrow 0 \equiv y^2 \equiv a \mod p$

$\times$ $p \nmid a$

Contradiction. So $y \not\equiv -y \mod p$

Q: How many quadratic residues mod p?

Thm: If p is an odd prime, then there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues mod p.

Pf: $f: \{1, 2, \ldots, p-1\} \longrightarrow \{1, 2, \ldots, p-1\}$

$x \longmapsto$ least pos. res. of x^2 mod p.

By prev. lemma, f is 2-to-1.

So image of f is half the size of the domain, i.e. $\frac{p-1}{2}$ elts.

Since image of f is the quadratic residues mod p, there are $\frac{p-1}{2}$ quadratic residues.

Every nonresidue mod p is nonzero

There are $p-1 - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic nonresidues mod p.

Legendre Symbol

Def: Let p be an odd prime and $a \in \mathbb{Z}$. The <u>Legendre symbol</u> $\left(\frac{a}{p}\right)$ is defined by

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

Thm (Euler's Criterion): If p is an odd prime and $a \in \mathbb{Z}$, then

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

Sanity check: if $p \nmid a$

Claim: $a^{\frac{p-1}{2}}$ is a sq. rt. of $1 \bmod p$.

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

Fermat's Little Thm.

Pf of Euler's Criterion:

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

Case 1: $p \mid a$

By def: $\left(\frac{a}{p}\right) = 0$

Also: $a^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} \equiv 0 \mod p$

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

Case 2: a is a quadratic residue mod p

By def: $\left(\frac{a}{p}\right) = 1$

$\exists\, x \in \mathbb{Z}$ with $p \nmid x$: $x^2 \equiv a \mod p$

$$\downarrow$$

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

$$1 \equiv x^{p-1} \equiv a^{\frac{p-1}{2}} \mod p$$

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

Case 3: a is a quadratic nonresidue mod p

By def: $\left(\frac{a}{p}\right) = -1$

Note: $\forall\ 1 \le i \le p-1.\ \exists\ 1 \le j \le p-1,\ j \ne i$

s.t. $ij \equiv a \mod p$

(given i, take $j \equiv i^{-1} a \mod p$)

$$-1 \equiv (p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)$$

$$\equiv a^{\frac{p-1}{2}} \mod p$$

Ex: Is 5 a quadratic residue mod 17?

Approach 1: Examine $1^2, 2^2, 3^2, \ldots, 8^2 \mod 17$ and see if any is $\equiv 5 \mod 17$.

$\hookrightarrow$ 8 multiplications

8 reductions mod 17

Approach 2: Euler's criterion

$$\left(\frac{5}{17}\right) \equiv 5^{\frac{17-1}{2}} \mod 17$$

$$= 5^8$$

$5^2 = 25 \equiv 8 \mod 17$

$5^4 \equiv 8^2 = 64 \equiv 13 \equiv -4 \mod 17$

$5^8 \equiv (-4)^2 \equiv 16 \equiv -1 \mod 17$

$\rightarrow \left(\frac{5}{17}\right) = -1 \longrightarrow$ 5 is not a quadratic residue mod 17

↳ 3 multiplications
3 reductions

Behavior of the Legendre Symbol:

Thm: 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 $\left(\frac{a^2}{p}\right) = 1$

Pf: ①, ③ ✓

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

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

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p$$

$$\underbrace{\left(\frac{ab}{p}\right)}_{\pm 1} \equiv \underbrace{\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)}_{\pm 1} \mod p$$

Since p odd, $1 \not\equiv -1 \mod p$

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

Cor: Modulo an odd prime p.

The product of two squares is a square

The product of a sq. and a non sq. is a non sq.

The product of two nonsqs. is a sq.

Q: When is -1 a square mod p?

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

$$(-1)^n = \begin{cases} 1 & n \text{ even} \\ -1 & n \text{ odd} \end{cases}$$

$$\frac{p-1}{2} \begin{cases} \text{even} & 4 \mid p-1 \\ \text{odd} & 4 \nmid p-1 \end{cases}$$

$$\frac{p-1}{2} \begin{cases} \text{even} & p \equiv 1 \mod 4 \\ \text{odd} & p \equiv 3 \mod 4 \end{cases}$$

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

$$\equiv \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

Fact: $\left(\frac{2}{p}\right) = 1$ if and only if

$$p \equiv \pm 1 \mod 8$$