$b^2 \pmod{n}$:

$\leftarrow n \rightarrow$

b ↓	5	6	7	8	9	10	11	12	13
1	1	1	1	1	1	1	1	1	1
2	4	4	4	4	4	4	4	4	4
3	4	3	2	1	0	9	9	9	9
4	1	4	2	0	7	6	5	4	3
5		1	4	1	7	5	3	1	12
6			1	4	0	6	3	0	10
7				1	4	9	5	1	10
8					1	4	9	4	12
9						1	4	9	3
10							1	4	9
11								1	4
12									1

modulo 13:

b	b'	b^2
1	1	1
2	2	4
3	3	9
4	4	3
5	5	12
6	6	10
7	-6	10
8	-5	12
9	-4	3
10	-3	9
11	-2	4
12	-1	1

Most values will appear at least twice: $b^2 = (-b)^2 \equiv_n (n-b)^2$.

What values appear as $b^2 \pmod{n}$?

i.e. what values a have square roots modulo n?

For now, sticking to prime modulus p:
Since

$$(p-b)^2 \equiv_p (-b)^2 = b^2,$$

we only need look at

$$b^2 \qquad \text{for } b = 1,\ 2,\ \ldots,\ \frac{p-1}{2}.$$

Let b be a integer that's not a multiple of p. Then if b is congruent to a square modulo p, we call it a quadratic residue (QR) modulo p. Otherwise, it's a (quadratic) nonresidue (NR) modulo p.

Ex: Modulo 13, the QRs are 1, 3, 4, 8, 10, and 12, a.k.a. $\pm 1, \pm 3$, and ± 4.

Theorem. Let p be an odd prime. Then there are exactly $(p-1)/2$ quadratic residues modulo p and exactly $(p-1)/2$ nonresidues modulo p. (Namely, there are as many residues as possible, which is half.)

Arithmetic with quadratic residues

QR × QR: Suppose a and a' are QRs modulo p.
Since $p \nmid a$ and $p \nmid a'$, we have $p \nmid aa'$.
So aa' is either a QR or a NR mod p.

But we have some b, b' such that $b^2 \equiv_p a$ and $(b')^2 \equiv_p a'$.
So $aa' \equiv_p b^2(b')^2 = (bb')^2$. Thus aa' is a QR as well.

QR × NR: Fix a a QR and a' a NR.
Since $p \nmid a$ and $p \nmid a'$, we have $p \nmid aa'$.
So aa' is either a QR or a NR mod p.
Moreover, we have some b such that $b^2 \equiv_p a$.

Now, if aa' is a QR, then there's some c such that $c^2 \equiv_p aa'$. So

$$c^2 \equiv_p aa' \equiv_p b^2 a'.$$

Now, since $a \not\equiv_p 0$, we have $b \not\equiv_p 0$ also. So $\gcd(b, p) = 1$, and therefore there's a multiplicative inverse b^{-1} modulo p. So

$$a' \equiv_p (b^{-1})^2 \cdot b^2 \cdot a' \equiv_p (b^{-1})^2 c^2 \equiv_p (b^{-1}c)^2,$$

which is a contradiction. So aa' is a NR.

Arithmetic with quadratic residues

NR × NR: Fix a a NR.
Consider

$$a,\ 2a,\ \ldots,\ (p-1)a \qquad \pmod p.$$

Since $p \nmid a$, we have $\gcd(a, p) = 1$, so as we showed in proving Fermat's Little Theorem, this list is just a rearrangement of

$$1,\ 2,\ \ldots,\ (p-1) \qquad \pmod p.$$

In particular, this list has the $(p-1)/2$ QRs and the $(p-1)/2$ NRs! But we showed that QR × NR = NR. So

$$\{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\} \quad \text{defined by} \quad x \mapsto ax \pmod p$$

sends the $(p-1)/2$ QRs to (distinct) NRs. Therefore, it *must* send the $(p-1)/2$ NRs all to QRs.

In other words, NR × NR = QR.

Arithmetic with quadratic residues: Legendre symbol

We have

QR × QR = QR   NR × QR = QR   NR × NR = QR.

Compare to

$$1 \times 1 = 1 \qquad 1 \times (-1) = -1 \qquad (-1) \times (-1) = 1.$$

The Legendre symbol of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR,} \\ -1 & \text{if } a \text{ is a NR,} \\ 0 & \text{if } a \text{ is a multiple of } p. \end{cases}$$

Theorem (Quadratic Residue Multiplication Rule)

Let p be a prime. Then

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

Spotting small QRs

If $p = 2$, then the possible residues are 0 and 1.
In particular, 1 is a QR. (Super easy case.)

Now, let p be an odd prime and fix $a \not\equiv_p 0$. Consider

$$A = a^{(p-1)/2} \quad \text{(reduced modulo } p\text{).}$$

Then $A^2 = a^{p-1} \equiv_p 1$. So

$$p | A^2 - 1 = (A+1)(A-1). \quad \text{So } p | A+1 \text{ or } p | A-1.$$

But $1 \leqslant A \leqslant p-1$. So $A = 1$ or $p-1$ (i.e. $A \equiv_p \pm 1$). Which one?

Spotting small QRs

$$A = a^{(p-1)/2} \quad \text{(reduced modulo } p\text{)}.$$

Theorem

If p is an odd prime then

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

Proof: First suppose $\left(\frac{a}{p}\right) \equiv_p 1$. Then there is some $b \not\equiv_p 0$ such that $b^2 \equiv_p a$. So

$$a^{(p-1)/2} \equiv_p (b^2)^{(p-1)/2} \equiv_p b^{p-1} \equiv 1 = \left(\frac{a}{p}\right).$$

Now consider the equation $x^N - 1 \equiv_p 0$ for $N = (p-1)/2$.
Since p is prime, there are at *most* $(p-1)/2$ solutions. Also, every one of the $(p-1)/2$ quadratic residues are solutions. So that's it! (Every non-residue is not a solution.)

$$\{\text{solns to } x^{(p-1)/2} - 1 \equiv_p 0\} = \{\text{quadratic residues modulo } p\}$$

Spotting small QRs

$$A = a^{(p-1)/2} \quad \text{(reduced modulo } p\text{)}.$$

Theorem

If p is an odd prime then

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

Proof: (continued) We have

$$\{\text{solns to } x^{(p-1)/2} - 1 \equiv_p 0\} = \{\text{quadratic residues modulo } p\}.$$

Now let $\left(\frac{a}{p}\right) = -1$ (i.e. a is a non-res). We saw before that

$$p | a^{(p-1)/2} + 1 \quad \text{or} \quad p | a^{(p-1)/2} - 1.$$

But $p \nmid a^{(p-1)/2} - 1$. So $p | a^{(p-1)/2} + 1$, i.e.

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

$\square$

Theorem

If p is an odd prime then

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

Let

$$A = a^{(p-1)/2} \qquad \text{(reduced modulo } p\text{)}.$$

Example:

Recall, modulo 13, the QRs are 1, 3, 4, 8, 10, and 12.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\left(\frac{a}{13}\right)$	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1
A	1	12	1	1	12	12	12	12	1	1	12	1

Theorem

If p is an odd prime then

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

Corollary (Quadratic reciprocity)

Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1, \\ -1 & \text{if } p \equiv_4 1. \end{cases}$$

Proof.

Compute $(-1)^{(p-1)/2} \pmod{p}$. □

$b^2 \pmod{p}$:

$\leftarrow p \rightarrow$

b	3	5	7	11	13
1	1	1	1	1	1
2	1	$\boxed{4}$	4	4	4
3		$\boxed{4}$	2	9	9
4		1	2	5	3
5			4	3	$\boxed{12}$
6			1	3	10
7				5	10
8				9	$\boxed{12}$
9				4	3
10				1	9
11					4
12					1

When is 2 a quadratic residue? (Read Chapter 21)

Let p be an odd prime, and let $P = \frac{p-1}{2}$.
Consider

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right) = 2^P P!.$$

On the other hand, consider the residues of $2, 4, 6, \ldots, p-1$ between $-P$ and P:

Ex: if $p = 7$, then $P = 3$, and

$$\{2, 4, 6\} \equiv_7 \{2, -3, -1\} = \{2\} \sqcup \{-1, -3\}.$$

Ex: if $p = 13$, then $P = 6$, and

$$\{2, 4, 6, 8, 10, 12\} \equiv_{13} \{2, 4, 6, -5, -3, -1\} = \{2, 4, 6\} \sqcup \{-1, -3, -5\}.$$

In general

$$\{2, 4, \ldots, p-1\} \equiv_p \{2, 4, \ldots, P\} \sqcup \{-1, -3, \ldots, -(P-1)\}.$$

So

$$2 \cdot 4 \cdots (p-1) \equiv_p (-1)^N P!, \quad \text{where } N = |\{-1, -3, \ldots, -(P-1)\}|.$$

So since $\gcd(P!, p) = 1$, we have $(-1)^N \equiv_p 2^P$.

When is 2 a quadratic residue? (Read Chapter 21)

Let p be an odd prime, and let $P = \frac{p-1}{2}$.
We have

$$(-1)^N \equiv_p 2^P \quad \text{where } N = |\{-1, -3, \ldots, -(P-1)\}|.$$

Theorem (Quadratic reciprocity, part 2)

Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv_8 \pm 1, \\ -1 & \textit{if } p \equiv_8 \pm 3. \end{cases}$$

Proof.

Compute N... □