April 14

Goal: Solve $ax^2+bx+c \equiv 0 \bmod n$ with $\gcd(2a,n)=1$

Over $\mathbb{Z}$: $ax^2+bx+c=0$

$\rightarrow x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

- two issues: division by $2a$
- is $\sqrt{b^2-4ac} \in \mathbb{Z}$

In $\mathbb{Z}/n\mathbb{Z}$: If $\gcd(2a,n)=1$, then division by $2a$ is not a problem

Main goal:
- does $\sqrt{b^2-4ac}$ exist mod n?
- what is it?

First step: Fix $a \in \mathbb{Z}$, p odd prime, $\gcd(a,p)=1$

Does $\sqrt{a}$ exist mod p i.e. does

$x^2 \equiv a \bmod p$

have a solution?

Example: $p=11$

$1^2 \equiv 1 \equiv 10^2$

$2^2 \equiv 4 \equiv 9^2$

$3^2 \equiv 9 \equiv 8^2$

$4^2 \equiv 5 \equiv 7^2$

$5^2 \equiv 3 \equiv 6^2$

So $x^2 \equiv 0 \bmod 11$ has one solution

$x^2 \equiv 1, 3, 4, 5, 9 \bmod 11$ has 2 solutions

↳ solutions are $x \equiv 5, 6 \bmod 11$ e.g.

$x^2 \equiv 2, 6, 7, 8, 10 \bmod 11$ has no solution

Notice: in $(\mathbb{Z}/11\mathbb{Z})^\times$ 5 squares

5 non squares

Definition

If $\gcd(a, p) = 1$ and $x^2 \equiv a \bmod p$ has a solution, then a is a quadratic residue modulo p. Otherwise a is a quadratic nonresidue

Definition

The Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a, \ a \text{ is a quad residue} \\ -1 & \text{if } p \nmid a, \ a \text{ is a quad nonres} \\ 0 & \text{if } p \mid a \end{cases}$$

Example

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

Ultimate goal here:

Theorem 9.9 Quadratic Reciprocity
Let p, q be distinct odd primes. Then

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

Auxiliary useful results

Theorem 9.6
If p is an odd prime

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,7 \bmod 8 \\ -1 & \text{if } p \equiv 3,5 \bmod 8 \end{cases}$$

Note: $\left(\frac{p}{2}\right) = 1$ if p is odd

We also already know

Theorem 5.5
If p is an odd prime

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

This was a consequence of Wilson's Thm.

The plan

① Properties of $\left(\frac{a}{p}\right)$ + computations using the Thms just mentioned

② Proof of Gauss's Lemma and its corollary

③ Proof of quadratic reciprocity

Computations:

Examples of application of QR

① We know $\left(\frac{7}{11}\right) = -1$

By QR, $\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1)^{\frac{11-1}{2}\frac{7-1}{2}}$

$$(-1)\left(\frac{11}{7}\right) = (-1)^{5\cdot 3} = -1$$

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

$\Rightarrow x^2 \equiv 11 \mod 7$ has a solution

yes: $x^2 \equiv 11 \equiv 4 \mod 7$

solutions are $x \equiv 2, 5 \mod 7$

② Compute $\left(\frac{3}{13}\right)$

We know by QR $\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = (-1)^{\frac{13-1}{2}\frac{3-1}{2}}$

$$\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = (-1)^{6\cdot 1} = 1$$

So $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right)$

But: $x^2 \equiv 13 \bmod 3$ is just $x^2 \equiv 1 \bmod 3$
This has solutions $x \equiv 1, 2 \bmod 3$
so $\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$

and $\left(\frac{3}{13}\right) = 1$ $x^2 \equiv 3 \bmod 13$ has 2 solutions

Example of some properties of Legendre symbol
We know $\left(\frac{9}{11}\right) = 1$ $\left(\frac{4}{11}\right) = 1$

$9 \cdot 4 = 36 \equiv 3 \bmod 11$ and $\left(\frac{3}{11}\right) = 1$

$$\left(\frac{9}{11}\right)\left(\frac{4}{11}\right) = \left(\frac{9\cdot 4}{11}\right) = \left(\frac{3}{11}\right)$$

a product of squares is a square. ok.

We know $\left(\frac{4}{11}\right)=1$ $\left(\frac{6}{11}\right)=-1$

$4\cdot 6=24\equiv 2 \bmod 11$ $\left(\frac{2}{11}\right)=-1$

$$\left(\frac{4}{11}\right)\left(\frac{6}{11}\right)=\left(\frac{4\cdot 6}{11}\right)=\left(\frac{2}{11}\right)=-1$$

a product of a square and a non square is a non square. ok.

We know $\left(\frac{2}{11}\right)=-1$ $\left(\frac{6}{11}\right)=-1$

$2\cdot 6=12\equiv 1 \bmod 11$ $\left(\frac{1}{11}\right)=1$

$$\left(\frac{2}{11}\right)\left(\frac{6}{11}\right)=\left(\frac{12}{11}\right)=\left(\frac{1}{11}\right)=1$$

a product of non squares is a square!!
that's not always true in $\mathbb{Z}$!!

also it looks like we can multiply the symbols?

Theorem 9.1: Euler's criterion

Let p be an odd prime, $\gcd(a,p)=1$. Then

$$\left(\frac{a}{p}\right)=1 \quad \text{iff} \quad a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

proof:

If $\left(\frac{a}{p}\right)=1$, there is x_0 with $x_0^2 \equiv a \bmod p$

Then $1 \equiv x_0^{p-1} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p$

↑ Fermat

Conversely if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, let r be a primitive root of p (always exists since p is an odd prime)

Then $a \equiv r^k \bmod p$ for some k

Then $a^{\frac{p-1}{2}} \equiv (r^k)^{\frac{p-1}{2}} \equiv 1 \bmod p$

Since r has order $p-1$, $p-1$ divides $\frac{k(p-1)}{2}$ i.e. $\frac{k}{2} \in \mathbb{Z}$ so k is even

So $(r^{k/2})^2 \equiv a \bmod p$

and $x_0 \equiv r^{k/2} \bmod p$ is a solution to $x_0^2 \equiv a \bmod p$. □

Theorem 9.2

Let p be odd, $\gcd(a,p)=\gcd(b,p)=1$. Then

a) If $a \equiv b \bmod p$,

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

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

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

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

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

proof

a) It is the same to solve

$x^2 \equiv a \bmod p$ or $x^2 \equiv b \bmod p$

if $a \equiv b \bmod p$

b) $x^2 \equiv a^2 \bmod p$ has solution $x \equiv a \bmod p$

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

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

so

$$a^{\frac{p-1}{2}} \equiv 1 \text{ or } -1 \bmod p$$

since those are the only 2 solutions to $x^2 \equiv 1 \bmod p$ (see the proof of Wilson's Thm)

So $a^{\frac{p-1}{2}} \equiv 1$ OR $-1 \bmod p$

If $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ then $\left(\frac{a}{p}\right) = 1$ by

Euler's criterion so $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$

If $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ then $\left(\frac{a}{p}\right) = -1$ by

Euler's criterion so again $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.

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

so $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$ but since the only values these take are ± 1 there is no "wrapping around" mod p and

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

e) $1 = 1^2$ so $\left(\frac{1}{p}\right) = 1$ by b)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

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

$\frac{p-1}{2}$ is even if $p \equiv 1 \bmod 4$ and odd if $p \equiv 3 \bmod 4$.

□

Corollary

Let r be a primitive root of p. Then the quadratic residues modulo p are

$$r^k \text{ with } k \text{ even}$$

and the non quadratic residues are

$$r^k \text{ with } k \text{ odd}$$

proof:

Recall that if r is a primitive root of p then any $a \in (\mathbb{Z}/p\mathbb{Z})$ is $a \equiv r^k \bmod p$, for some $k \in \mathbb{Z}/(p-1)\mathbb{Z}$, so the corollary covers every element of $(\mathbb{Z}/p\mathbb{Z})^\times$

Now by Euler's criterion,

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

If k is even, $k = 2\ell$, then $(r^{2\ell})^{\frac{p-1}{2}} = (r^\ell)^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem

If k is odd, $k = 2\ell+1$ then
$(r^{2\ell+1})^{\frac{p-1}{2}} = (r^\ell)^{p-1} r^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \not\equiv 1 \mod p$
since r has order $p-1$ and $0 < \frac{p-1}{2} < p-1$.

So $\left(\frac{r^k}{p}\right) \equiv r^{\frac{p-1}{2}} \equiv -1 \mod p$ in that case

□

Theorem 9.4
If p is an odd prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ contains $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non residues

proof: Consider r^k for r a primitive root and $0 \le k \le p-2$ (this gives all of $(\mathbb{Z}/p\mathbb{Z})^\times$)
Half of the k's are even and half are odd since $p-2$ is odd.

□