Note: $\sum_{d|n}$ means the sum is taken over all divisors of n.

E.g. $\sum_{d|6} \frac{1}{d} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$

Squares mod p

- Determine when a quadratic congruence has a soln or not.

Legendre Symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a = \square \bmod p \\ -1 & a \neq \square \bmod p \\ 0 & \gcd(a,p) \neq 1 \end{cases}$$

Key Properties:

- $\left(\frac{a}{p}\right)$ depends only on the class of $a \bmod p$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}$
- $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1,7 \bmod 8 \\ -1 & p \equiv 3,5 \bmod 8 \end{cases}$
- $\left(\frac{a}{p}\right) \equiv a^{p-1/2} \bmod p$

↑

Euler's Criterion

Quadratic Reciprocity:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{1}{p}\right) & \text{at least one of } p \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{1}{p}\right) & \text{both of } p \text{ or } q \equiv 3 \bmod 4 \end{cases}$$

Another way to write this:

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

Ex: $\left(\frac{79}{101}\right) \overset{QR}{=} \left(\frac{101}{79}\right) = \left(\frac{22}{79}\right)$

$= \left(\frac{2}{79}\right)\cdot\left(\frac{11}{79}\right)$

$$\left(\frac{2}{79}\right) = 1$$

$$\left(\frac{11}{79}\right) \overset{QR}{=} -\left(\frac{79}{11}\right) = -\left(\frac{2}{11}\right) = -(-1) = 1.$$

$$\Rightarrow \left(\frac{79}{101}\right) = 1.$$

One application of QR: given a, for what primes p does $a \equiv \square \bmod p$?

Ex: For what p is 15 a square mod p?

$$\left(\frac{15}{p}\right) = 1 \ ?$$

$$\left(\frac{15}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{5}{p}\right)$$

need either both to be 1 or both to be -1.

Since $5 \equiv 1 \bmod 4$,

$$\left(\frac{5}{p}\right) \overset{QR}{=} \left(\frac{p}{5}\right).$$

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & p \equiv 1,4 \bmod 5 \\ -1 & p \equiv 2,3 \bmod 5 \end{cases}$$

To compute $\left(\frac{3}{p}\right)$, case on p mod 4:

$p \equiv 1 \bmod 4$:

$$\left(\frac{3}{p}\right) \overset{QR}{=} \left(\frac{p}{3}\right)$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 3 \\ -1 & p \equiv 2 \bmod 3 \end{cases}$$

$p \equiv 3 \bmod 4$

$$\left(\frac{3}{p}\right) \overset{QR}{=} -\left(\frac{p}{3}\right)$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 2 \bmod 3 \\ -1 & p \equiv 1 \bmod 3 \end{cases}$$

Now piece everything together:

$p \equiv 1 \bmod 4$:

$p \equiv 1 \bmod 3$ + +

$p \equiv 1, 4 \bmod 5$

$p \equiv 2 \bmod 3$ − −

$p \equiv 2, 3 \bmod 5$

We get 4 possible

Systems of Congruence Equations:

$p \equiv 1 \mod 4$
$p \equiv 1 \mod 3$
$p \equiv 1 \mod 5$

$p \equiv 1 \mod 4$
$p \equiv 1 \mod 3$
$p \equiv 4 \mod 5$

$p \equiv 1 \mod 4$
$p \equiv 2 \mod 3$
$p \equiv 2 \mod 5$

$p \equiv 1 \mod 4$
$p \equiv 2 \mod 3$
$p \equiv 3 \mod 5$

Can solve each System w/ CRT.

$p \equiv 1, 49, 17, 53 \mod 60$.

$p \equiv 3 \mod 4$:

$p \equiv 2 \mod 3$ $\quad + +$

$p \equiv 1, 4 \mod 5$

$p \equiv 1 \mod 3$ $\quad - -$

$p \equiv 2, 3 \mod 5$

Again, get 4 congruences

to solve w/ CRT.

$p \equiv 11, 59, 7, 43 \mod 60.$

Putting this together:

$p \equiv 1, 7, 11, 17, 43, 49, 53, 59 \mod 60.$

Generalization of

Legendre Symbol: Jacobi Symbol.

$n = p_1^{e_1} \cdots p_k^{e_k}$ p_i odd

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

↑ Jacobi Symbol

Key Properties:

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

- $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

- $\left(\frac{-1}{n}\right) = \begin{cases} 1 & n \equiv 1 \pmod 4 \\ -1 & n \equiv 3 \pmod 4 \end{cases}$

- $\left(\frac{2}{n}\right) = \begin{cases} 1 & n \equiv 1,7 \pmod 8 \\ -1 & n \equiv 3,5 \pmod 8 \end{cases}$

- $\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{n}\right)$ if $(n,m) = 1$.

i.e. $\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{n}{m}\right) & \text{at least one of } n,m \equiv 1 \bmod 4 \\ -\left(\frac{n}{m}\right) & \text{both } n,m \equiv 3 \bmod 4 \end{cases}$

Jacobi Reciprocity

WARNING: $\left(\frac{a}{n}\right) = 1$

does not mean that $a = \square \bmod n$.

e.g. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$

but $2 \neq \square \bmod 15$.

However, if $a = \square \bmod n$ then $\left(\frac{a}{n}\right) = 1$, and equivalently,

if $\left(\frac{a}{n}\right) = -1$ then $a \neq \square \bmod n$.

Ex: $\left(\frac{28}{45}\right) = \left(\frac{2^2 \cdot 7}{3^2 \cdot 5}\right)$

$$= \left(\frac{2^2 \cdot 7}{3}\right)^2 \cdot \left(\frac{2^2 \cdot 7}{5}\right)$$

$$= \left(\frac{2}{5}\right)^2 \cdot \left(\frac{7}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Jacobi Symbol is <u>much</u> more efficient for computing Legendre Symbols.

<u>Ex:</u> $\left(\frac{1001}{9907}\right)$

If we use Legendre Symbols:

$1001 = 7 \cdot 11 \cdot 13$

$$\left(\frac{7}{9907}\right) \cdot \left(\frac{11}{9907}\right) \cdot \left(\frac{13}{9907}\right)$$

$$\left(\frac{7}{9907}\right) \overset{QR}{=} -\left(\frac{9907}{7}\right) = -\left(\frac{2}{7}\right) = -1$$

$$\left(\frac{11}{9907}\right) \overset{QR}{=} -\left(\frac{9907}{11}\right) = -\left(\frac{7}{11}\right)$$

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

$$\left(\frac{13}{9907}\right) \overset{QR}{=} \left(\frac{9907}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

So $\left(\frac{1001}{9907}\right) = -1.$

Using Jacobi Symbols:

$$\left(\frac{1001}{9907}\right) \overset{JR}{=} \left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right)$$

$$= \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right)$$

$$\left(\frac{2}{1001}\right) = 1$$

$$\left(\frac{449}{1001}\right) \overset{JR}{=} \left(\frac{1001}{449}\right) = \left(\frac{103}{449}\right)$$

$$\overset{JR}{=} \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) \overset{JR}{=} \left(\frac{103}{37}\right)$$

$$= \left(\frac{29}{37}\right) \overset{JR}{=} \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right)$$

$$= \left(\frac{2}{29}\right)^3 = (-1)^3 = -1.$$