Quadratic Reciprocity

$p \neq q$ $\quad$ p, q odd primes

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

We will prove this using <u>Gauss sums</u>.

$$\omega = e^{2\pi i/p} \qquad \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \omega^k$$

Thm: Let $p>2$ be prime & let ω be a primitive pth root of unity. Then

$$g_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \omega^k = \begin{cases} \pm\sqrt{p} & p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & p \equiv 3 \pmod 4 \end{cases}$$

Suffices to show $g_p^2 = \left(\frac{-1}{p}\right) p$

$$g_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) w^k = \sum_{k=0}^{p-1} \left(k/p\right) w^k$$

$$g_p^2 = \left(\sum_{k=0}^{p-1} \left(\frac{k}{p}\right) w^k \right)^2$$

$$= \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \left(j/p\right)\left(k/p\right) w^{j+k}$$

$$g_p^2 = a_0 + a_1 w + a_2 w^2 + \cdots + a_{p-1} w^{p-1}$$

$$a_n = \sum_{\substack{j+k \equiv n \\ (\mathrm{mod}\ p)}} \left(j/p\right)\left(k/p\right)$$

$$a_0 = \sum_{\substack{j+a \equiv 0 \\ (\mathrm{mod}\ p)}} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) = \sum_{j=0}^{p-1} \left(\frac{-j}{p}\right)\left(\frac{j}{p}\right)$$

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

$$= \begin{cases} 0 & j = 0 \\ \left(\frac{-1}{p}\right) & \text{Otherwise} \end{cases}$$

$$\boxed{a_0 = \left(\frac{-1}{p}\right)(p-1)}$$

$$n \neq 0 \quad a_n = \sum_{\substack{j+k \equiv n \\ (\text{mod } p)}} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right)$$

$$j \equiv nj' \qquad k \equiv nk' \qquad j'+k' \equiv 1 \ (\text{mod } p)$$

$$a_n = \sum_{\substack{j'+k' \equiv 1 \\ (\text{mod } p)}} \left(\frac{nj'}{p}\right)\left(\frac{nk'}{p}\right)$$

$$\left(\frac{nj'}{p}\right)\left(\frac{nk'}{p}\right) = \left(\frac{n^2}{p}\right)\left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right)$$

$$= \left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right)$$

$$a_n = \sum_{\substack{j'+k' \equiv 1 \\ (\bmod p)}} \left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right) = a_1$$

$$\boxed{a_1 = a_2 = a_3 = \cdots = a_{p-1}}$$

We will now show that

$$a_0 + a_1 + \cdots + a_{p-1} = 0$$

Think of g_p as a polynomial in x

$$g_p(x) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) x^k$$

$$g_p(1) = \sum_{k=0}^{p-1} (k/p) = 0 \qquad g_p(1)^2 = 0$$

$g_p(1)^2$ is sum of coefficients in $g_p(x)^2$

So, $a_0 + a_1 + \cdots + a_{p-1} = 0$

$a_1 = a_2 = \cdots = a_{p-1}$

$a_0 = \left(-1/p\right)(p-1)$

$$\left(\frac{-1}{p}\right)(p-1) + (p-1)a_1 = 0$$

$$a_1 = \left(\frac{-1}{p}\right)$$

$$g_p^2 = \sum_{k=0}^{p-1} a_k \omega^k$$

$$= \left(\frac{-1}{p}\right)\left((p-1) - \omega - \omega^2 - \omega^3 - \dots - \omega^{p-1}\right)$$

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

Call $\left(\frac{-1}{p}\right) p = p^*$

Proof of quadratic reciprocity

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

or

$$\left(q/p\right) = \left(p^*/q\right)$$

$$g_p^2 = p^*$$

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

$$\equiv \left(\frac{p^*}{q} \right) \pmod q$$

$$g_p^q \equiv \left(\frac{p^*}{q} \right) g_p \pmod q$$

$$g_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) w^k$$

Mod q

$$(g_p)^q \equiv \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) w^{qk}$$

Let a be such $aq \equiv 1 \pmod p$; $t = qk$

$$(g_p)^q \equiv \left(\frac{a}{p}\right) \sum_{k=1}^{p-1} \left(\frac{t}{p}\right) w^t$$

$$\equiv \left(\frac{q}{p}\right) g_p \pmod q$$

$$(g_p)^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q}$$

So

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

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

Is 5 a square mod 101?

→ Evaluate $(5)^{50} \pmod{101}$

OR

→ Consider multiplication by 5 and take sign of that permutation

OR

$$\left(\frac{5}{101}\right)\left(\frac{101}{5}\right) = (-1)^{(2)(50)} = 1$$

$\left(\frac{101}{5}\right)$ is easier to evaluate

$$\left(\frac{101}{5}\right) = \left(1/5\right) = 1$$

So 5 is a square modulo 101.

Qn: For what primes p, is $\left(3/p\right) = 1$?

$$\left(3/p\right) = \left(p/3\right)(-1)^{p-1/2}$$

$\left(\frac{p}{3}\right)$ Depends on $p \pmod 3$

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

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

$$\left.\begin{aligned} p &\equiv 1 \pmod{3} \\ p &\equiv 1 \pmod{4} \end{aligned}\right\} \Rightarrow p \equiv 1 \pmod{12}$$

$$\left.\begin{aligned} p &\equiv 1 \pmod{3} \\ p &\equiv -1 \pmod{4} \end{aligned}\right\} \Rightarrow p \equiv 7 \pmod{12}$$

$$\left.\begin{aligned} p &\equiv -1 \pmod{3} \\ p &\equiv 1 \pmod{4} \end{aligned}\right\} \Rightarrow p \equiv 5 \pmod{12}$$

$$\left.\begin{aligned} p &\equiv -1 \pmod{3} \\ p &\equiv -1 \pmod{4} \end{aligned}\right\} \Rightarrow p \equiv 11 \pmod{12}$$

Combine everything

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$$