To prove cubic reciprocity, need slightly more general set-up.

Given any mult. hom. $\chi : G \longrightarrow \mathbb{C}^*$, G : finite gp.

$\mathbb{C}^*$: non-zero cx. #'s.

$(\chi(ab) = \chi(a)\chi(b))$

call this **character**. For us, consider $(\mathbb{Z}/p\mathbb{Z})^\times$, ok.

Definition implies nice properties:

(I) $\chi(1) = 1$. (since $\chi(a \cdot 1) = \chi(a) \cdot \chi(1)$ for all $a \in G$.)

(II) $\chi(a)$ is a root of unity.

(since $a^{|G|} = 1$, in any gp. $\chi(a^{|G|}) = \chi(a)^{|G|}$; $\chi(a^{|G|}) = \chi(1) = 1 \Rightarrow \chi(a)^{|G|} = 1$)

(III) $\chi(a^{-1}) = \overline{\chi(a)}$.

examples: residue symbols., triv. char. mod p.

Facts about characters: (A) if χ non-trivial, on $\mathbb{Z}/p\mathbb{Z}$

then $\displaystyle\sum_{t \pmod p} \chi(t) = 0$.

(B) Mult. chars form a gp., cyclic of order $p-1$.

(C) $\displaystyle\sum_{\chi : \text{char}} \chi(a) = 0$ for any $a \neq 1$.

then define Gauss sums for any char. χ mod p.

$$g(a,\chi) \overset{\text{def}}{=} \sum_t \chi(t)\,\xi^{at}. \qquad \xi = e^{2\pi i/p}, \text{ as usual.}$$

then all same properties hold:

- if $a \neq 0$, χ non-triv. $\quad g(a,\chi) = \chi(a^{-1})\, g(1,\chi)$

$$\left(\begin{array}{ll} a\neq 0, \chi \text{ triv.} & g(a,\chi) = 0. \\ a = 0, \chi \text{ non-triv} & g(a,\chi) = 0 \\ a = 0, \chi \text{ triv.} & g(a,\chi) = p \end{array}\right)$$

- if χ non-triv., $|g(\chi)| = \sqrt{p}$. (same pfs as before)

Additional sum using characters: Jacobi sum.

$$J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b) \qquad \chi,\lambda \text{ chars. mod } p.$$

Motivation: Find # of solutions to $(x^2+y^2 \equiv 1) \pmod p$

claim: $$\#(x^2+y^2\equiv 1) = \sum_{\substack{a+b=1 \\ a,b}} \#(x^2\equiv a)\,\#(y^2\equiv b)$$

But $$\#(x^2\equiv a) = \left(1 + \left(\frac{a}{p}\right)\right)$$

i.e. $$\#(x^2+y^2\equiv 1) = \sum_{a+b=1} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right)$$

$$= \sum_{a+b=1} 1 + \left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$= p + \sum_a \underbrace{\left(\frac{a}{p}\right)}_{0} + \sum_b \underbrace{\left(\frac{b}{p}\right)}_{0} + \sum_{a+b=1} \underbrace{\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)}_{J(\chi_p, \chi_p)}$$

$\uparrow$ Legendre symb. mod p.

try it on your own for

$$\#\left(x^3 + y^3 \equiv 1 \right) \pmod{p}.$$

express answer using Jacobi sums.

Gauss sums and Jacobi sums are related.

Facts about Jacobi sums: ✓ all characters for $\mathbb{Z}/p\mathbb{Z}$.

(I) $J(1_p, 1_p) = p$

(II) $J(1_p, \chi) = 0$

(III) $J(\chi, \chi^{-1}) = -\chi(-1)$

(IV) if $\chi \cdot \lambda \neq 1_p$, then

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

parts (III) & (IV) take some work.

(IV): write out definition of $g(\chi)g(\lambda)$ and then change vars. in summation.

$$(x,y) \longmapsto \sum_t \sum_{x+y=t}$$

cases: $t=0$, $t \neq 0$.

(Cor. of IV): $|J(\chi,\lambda)| = \sqrt{p}$.

since $|g(\chi)| = |g(\lambda)| = |g(\chi,\lambda)| = \sqrt{p}$.

Generalization of (IV): if $p \equiv 1 \ (n)$, χ : char. of order $n > 2$. Then

$$g(\chi)^n = \chi(-1) \cdot p \cdot J(\chi,\chi)\, J(\chi,\chi^2) \cdots J(\chi,\chi^{n-2})$$

(follows from repeated application of (IV): $\chi \overset{w/}{=} \lambda$

$$g(\chi)^2 = J(\chi,\chi)\, g(\chi^2), \quad g(\chi)^3 = J(\chi,\chi^2)\, J(\chi,\chi)\, g(\chi^3)$$

(after mult. by $g(\chi)$ on both sides, using recip. of IV)

As special case, $\boxed{g(\chi)^3 = p \cdot J(\chi,\chi)}$ (since $\chi(-1) = 1$.)

FACT B: if $p \equiv 1 \ (3)$, χ : cubic. $J(\chi,\chi) = a + b\omega$, $\omega^3 = 1$,

then $J(\chi,\chi)$ has $b \equiv 0 \ (3)$, $a \equiv 2 \ (3)$.

(prove this using fact in box above, +

$$g(\chi)^3 \equiv -1 \ (3), \quad g(\bar{\chi})^3 \equiv -1 \ (3)$$

i.e. $a + b\omega \equiv -1 \ (3)$, $a + b\bar{\omega} \equiv -1 \ (3)$

$\Rightarrow$ $b(\omega - \bar{\omega}) \equiv 0 \ (3)$ i.e. $b \cdot \sqrt{-3} \equiv 0 \ (3)$

$-b^2 \cdot 3 \equiv 0 \ (9)$

$\Rightarrow 3 \mid b$.

So $a + b\omega \equiv -1 \ (3)$

$\Rightarrow a \equiv -1 \ (3)$ ✓.)

But we know $|J(\chi,\chi)| = \sqrt{p}$, so in part. (this true if $\chi \cdot \lambda \neq 1_p$)

$|J(\chi,\chi)|^2 = p$ for χ : cubic

so $J(\chi,\chi) = a + b\omega$ is a primary prime in $\mathbb{Z}[\omega]$ of norm p.

(if $p \equiv 1 \ (3)$)

Sneaky part: if π prime in $\underset{\parallel}{R} \mathbb{Z}[\omega]$, $N(\pi) = p \equiv 1 \ (3)$,

then $R/\pi R$ has p elements $\{0, 1, \cdots, p-1\}$.

(isomorphic to $\mathbb{Z}/p\mathbb{Z}$). So the cubic residue symbol $\left(\frac{\cdot}{\pi}\right)_3 =: \chi_\pi$

may be considered (via isom.) as character on $\mathbb{Z}/p\mathbb{Z}$.

Can consider $g(a, \chi_\pi)$, $J(\chi_\pi, \chi_\pi)$ with same props. as before.

In part., $J(\chi_\pi, \chi_{\bar{\pi}})$ is primary prime with norm p.

Claim: $J(\chi_\pi, \chi_{\bar{\pi}}) = \pi$. (Assume π primary here)

Suppose $J(\chi_\pi, \chi_{\bar{\pi}}) = \pi'$, with $\pi' \bar{\pi}' = p = \pi\bar{\pi}$

$\Rightarrow$ $\pi \mid \pi'$ or $\pi \mid \bar{\pi}'$. (actually since all primes are primary

$\pi = \pi'$ or $\pi = \bar{\pi}'$)

enough to show $J(\chi_\pi, \chi_\pi) \equiv 0 \ (\pi)$.

But $J(\chi_\pi, \chi_\pi) = \sum_{\alpha \in \mathbb{Z}/p\mathbb{Z}} \chi_\pi(\alpha)\chi_\pi(1-\alpha) \equiv \sum_{\alpha \in \mathbb{Z}/p\mathbb{Z}} \alpha^{p-1/3}(1-\alpha)^{p-1/3} \quad (\pi)$

claim $\overset{\text{RHS}}{\equiv} 0 \ (p)$, hence $\equiv 0 \ (\pi)$. ✓

Corollary: $g(\chi_\pi)^3 = p \cdot \pi$. ($\pi$: primary prime, $N(\pi) \equiv 1 \ (3)$)

pf. of CR: Know $g(\chi_\pi)^3 = p\pi$. Let $q \equiv 2 \pmod 3$, another prime.

$$\Rightarrow \quad \left(g(\chi_\pi)^3\right)^{q^2-1/3} = (p\pi)^{q^2-1/3} \equiv \chi_q(p\pi) \pmod{q}.$$

But $q \equiv 2 \pmod 3 \Rightarrow \chi_q(p) = 1$. i.e.

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi) \cdot g(\chi_\pi) \pmod{q}. \qquad (*)$$

LHS:
$$= \left(\sum_t \chi_\pi(t)\,\zeta^t\right)^{q^2} \equiv \sum_t \left(\chi_\pi(t)\right)^{q^2} \zeta^{q^2 t} \pmod{q}$$

but $q^2 \equiv 1 \pmod 3$ so $\chi_\pi(t)^{q^2} = \chi_\pi(t)$.
$$= \sum_t \chi_\pi(t)\,\zeta^{q^2 t} = g(q^2, \chi_\pi).$$

$$g(q^2, \chi_\pi) = \chi_\pi(q^2)^{-1}\, g(\chi_\pi)$$
$$= \chi_\pi(q)\; g(\chi_\pi).$$

Combining w/ $(*)$ gives $\chi_\pi(q)\, g(\chi_\pi) \equiv \chi_q(\pi)\, g(\chi_\pi) \pmod{q}$.

Now mult. both sides by $\overline{g(\chi_\pi)}$, get $g(\chi_\pi)\,\overline{g(\chi_\pi)} = p$. cancel.

(case with both π_1, π_2 with $N(\pi_1) \equiv N(\pi_2) \equiv 1 \pmod 3$ similar).