

1

Quadratic reciprocity

1 Proof (inspired by Serre)

Definition 1. The *Legendre symbol* $\left(\frac{a}{p}\right)$, where p is an odd prime, and a is any integer is equal to $+1$ if a has a square root in $\mathbb{Z}/p\mathbb{Z}$, and -1 otherwise.

Our goal is

Theorem 2. (Legendre, Gauss) If p and q are two odd primes, then

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

Proof. Write $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$. We will work in the subring $\mathbb{Z}[\zeta] \subseteq \mathbb{C}$. This is just the ring made of all polynomials in ζ .

Let's consider the so-called "Gauss sum"

$$\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) \zeta^a$$

It has many nice properties:

- First property: $\left(\frac{-1}{p}\right) \cdot \tau^2 = p$
 Indeed, one has $\left(\frac{-1}{p}\right) \cdot \tau^2 = \left(\frac{-1}{p}\right) \cdot \sum_{a,b} \left(\frac{a \cdot b}{p}\right) \zeta^{a+b} = \sum_{a,b} \left(\frac{a \cdot (-b)}{p}\right) \zeta^{a+b}$,
 because $\left(\frac{c}{p}\right) \cdot \left(\frac{d}{p}\right) = \left(\frac{c \cdot d}{p}\right)$. One also has that $\left(\frac{c}{p}\right) = \left(\frac{c^{-1}}{p}\right)$ (because c has a square root if and only if its inverse has one).
 Thus $\sum_{a,b} \left(\frac{a \cdot (-b)}{p}\right) \zeta^{a+b} = \sum_{a,b} \left(\frac{a \cdot b}{p}\right) \zeta^{a-b} = \sum_{a,b} \left(\frac{a \cdot b^{-1}}{p}\right) \zeta^{a-b} = \sum_{c,b} \left(\frac{c}{p}\right) \zeta^{b \cdot c - b}$,
 just thanks to the change of variables $c = a \cdot b^{-1}$.
 At this point, one can break the last sum in two groups ($c = 1$) and ($c \neq 1$) and get

$$\left(\frac{-1}{p}\right) \cdot \tau^2 = \left(\frac{1}{p}\right) \cdot \sum_b 1 + \left(\sum_{c \neq 1} \left(\frac{c}{p}\right)\right) \cdot \sum_{b \neq 0} (\zeta^{c-1})^b = (p-1) + (-1) \cdot (-1) = p.$$

Indeed: $\left(\frac{1}{p}\right) = 1$, always, and $\sum_c \left(\frac{c}{p}\right) = 0$, because there are as many elements that have a square root as elements that do not have a square root (multiply the first set by one element in the second set to get everybody in the second set!), and so $1 + \sum_{c \neq 1} \left(\frac{c}{p}\right) = 0$. Now the last part is well-known to you: the sum of the n -th roots of unity is always zero.

- Second property: $\tau^q = \tau \cdot (\tau^2)^{\frac{p-1}{2}} = \tau \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \pmod{p}$.
 Just use the first property and remember that $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}$ (We saw that earlier).
- Third property: $\tau^q = \left(\frac{q}{p}\right) \cdot \tau \pmod{q}$
 Indeed if you remember that in $\mathbb{Z}/q\mathbb{Z}$ one has $(x+y)^q \equiv x^q + y^q$, then

$$\tau^q = \sum_a \left(\frac{a}{p}\right)^q \cdot \zeta^{a \cdot q} = \sum_a \left(\frac{a}{p}\right) \cdot \zeta^{a \cdot q} = \sum_a \left(\frac{a \cdot q^2}{p}\right) \cdot \zeta^{a \cdot q} = \left(\frac{q}{p}\right) \cdot \sum_a \left(\frac{a \cdot q}{p}\right) \cdot \zeta^{a \cdot q} = \left(\frac{q}{p}\right) \cdot \tau$$

Basically, $\left(\frac{q^2}{p}\right) = 1$, and since q is odd, $\left(\frac{a}{p}\right)^q = (\pm 1)^q = \pm 1$ which explains the line above.

Now we are done! Just put together property 2 and 3 (and remember that $p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right)$).

□