16 The Quadratic Reciprocity Law

Fix an odd prime p. If q is another odd prime, a fundamental question, as we saw in the previous section, is to know the sign $\left(\frac{q}{p}\right)$, i.e., whether or not q is a square mod p. This is a very hard thing to know in general. But Gauss noticed something remarkable, namely that knowing $\left(\frac{q}{p}\right)$ is equivalent to knowing $\left(\frac{p}{q}\right)$; they need not be equal however. He found the precise law which governs this relationship, called the *Quadratic Reciprocity Law.* Gauss was very proud of ths result and gave several proofs. We will give one of his proofs, which incidentally introduces a very basic, ubiquitous sum in Mathematics called the *Gauss sum.* We will also give an alternate proof, which is in some sendse more clever than the first, due to Eisenstein.

Theorem (Gauss) (Quadratic reciprocity) *Let p, q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{p}{q}\right).$$

Explicitly,

$$(q/p)/(p/q) = \begin{cases} 1, & \text{if } p \text{ or } q \text{ is } \equiv 1 \pmod 4 \\ -1, & \text{if } p \textbf{ and } q \text{ are } \equiv 3 \pmod 4 \end{cases}$$

This theorem is very useful in computations.

Example

$$\left(\frac{37}{691}\right) = 3$$

It is not easy to compute $(37)^{\frac{691-1}{2}} \pmod{691}$.

Better to use then:

$$\begin{aligned}
\left(\frac{37}{691}\right) &= \underbrace{(-1)^{\left(\frac{37-1}{2}\right)\left(\frac{691-1}{2}\right)}}_{1} \left(\frac{691}{37}\right) \\
&= \left(\frac{691}{37}\right); \ \frac{691}{37} = 18\,\frac{25}{37} \\
&= \left(\frac{25}{37}\right) = \left(\frac{5}{37}\right)^2 = 1
\end{aligned}$$

Proof # 1 of theorem: p, q odd primes, $p \neq q$. Put

$$\xi = e^{\frac{2\pi i}{q}} \in \mathbb{C}$$

Then

$$\xi^q = 1, \text{ but } \xi^m \neq 1 \text{ if } m < q.$$

ξ is called a primitive qth root of unity in $\mathbb{C}$. All powers of ξ will be on the unit circle. In fact, we get a regular q-gon by converting the point

$$1, \xi, \ldots, \xi^{q-1}$$

cyclotong = "circle division"

Put $R = \{\alpha = a_0 + a_1\xi + \cdots + a_{\xi-1}\xi^{q-1} | a_0, a_1, \ldots, a_{q-1} \in \mathbb{Z}\}$. Clearly, $R \supset \mathbb{Z}$, hence R has 0×1. Let

$$\alpha = \sum_{i=1}^{q-1} a_i q^{\xi}, \ \beta = \sum_{i=1}^{q-1} b_i q^{\xi}$$

be in R. Then

$$\alpha \pm \beta = \sum_{i=1}^{q-1} (a_i + b_i)\xi^i \in R.$$

Since $\xi^q = 1$, given any $n \in \mathbb{Z}$ we can write $n = \ell q + r$, $0 \leq r \leq q - 1$ by Euclidean algorithm in $\mathbb{Z}$, and conclude that

$$\xi^n = \xi^r.$$

So R contains all the integral powers of ξ. Then it also contains finite integral linear combinations of such powers. Consequently,

$$\alpha\beta \in R \text{ if } \alpha, \beta \in R.$$

So R is very much like $\mathbb{Z}$. It is a q-dimensional analog of $\mathbb{Z}$. This allows us to define the divisibility in R. To be precise, if $\alpha, \beta \in R$, we say that β divides α, $\beta | \alpha$ iff $\exists \gamma \in R$ such that $\alpha = \beta\gamma$.

In particular, $R \ni p$, and it makes sense to ask if p divides some number in R.

Definition: Let $\alpha, \beta \in R$. We say that

$$\alpha \equiv \beta \pmod{p} \text{ iff } p | (a - b) \text{ in } R.$$

This allows us to do "congruence arithmetic" mod p in R.

To study $(\frac{q}{p})$, Gauss introduced the following "Gauss Sum":

$$S_q = \sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^a.$$

Clearly, $S_q \in R$.

Aside (Not part of proof of Quad. Recip., but interesting)

$$S_q = \sum_{a=1}^{\frac{q-1}{2}} \left(\left(\frac{a}{q}\right) \xi^a + \underbrace{\left(\frac{-a}{q}\right) \xi^{-a}}_{(\frac{-1}{q})(\frac{a}{q})\bar{\xi^a}} \right)$$

So if

$$\left(\frac{-1}{q}\right) = 1,\ S_q = \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{a}{q}\right) (\xi^a + \bar{\xi^a}) \in R \cap \mathbb{R}$$

and if

$$\left(\frac{-1}{q}\right) = -1,\ S_q \in R \cap i\mathbb{R}$$

pure read or im.

Lemma 1:

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

Proof of Lemma 1:

$$\begin{aligned} S_q^2 &= \left(\sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^a \right) \left(\sum_{b \bmod q} \left(\frac{b}{q}\right) \xi^b \right) \\ &= \sum_{a \bmod q} \sum_{b \bmod q} \left(\frac{a}{q}\right) \left(\frac{b}{q}\right) \xi^a \xi^b \\ &= \sum \sum \left(\frac{ab}{q}\right) \xi^{a+b} \\ &= \sum_{c \bmod q} \xi^c \left(\sum_{a \bmod q} \left(\frac{a(c-a)}{q}\right) \right) \end{aligned}$$

So

$$S_q^2 = \sum_{c \bmod q} \xi^c \sum_{a \bmod q} \left(\frac{ac - a^2}{q}\right)$$
$$= \sum_{c \bmod q} \xi^c \sum_{a \bmod q} \left(\frac{-a^2(1 - a'c)}{q}\right),$$

where $a'a \equiv 1 \pmod q$.

But

$$\left(\frac{-a^2(1-a'c)}{q}\right) = \underbrace{\left(\frac{-1}{q}\right)}_{(-1)^{\frac{q-1}{2}}} \underbrace{\left(\frac{a^2}{q}\right)}_{=1 \text{ as } a \equiv 0 \bmod q} \left(\frac{1-a'c}{q}\right)$$

$$\Rightarrow S_q^2 = (-1)^{\frac{q-1}{2}} \sum_{c \bmod q} \xi^c f(c),$$

where

$$f(c) = \sum_{a \bmod q} \left(\frac{1-a'c}{q}\right) \quad a \not\equiv 0 \bmod q$$

$f(c) = ?$

c ≡ 0 (mod q):

$$f(0) = \sum_{\substack{a \bmod q \\ a \not\equiv 0 \pmod q}} \left(\frac{1}{q}\right)$$
$$\Rightarrow f(0) = q - 1$$

c ≢ 0 (mod q): Note that, in this case, the set

$$\{1 - a'c | a \bmod q,\ a \not\equiv 0 \bmod q\}$$

runs over elements of $\mathbb{Z}/q - \{1\}$ exactly once. Indeed, given any $b \in \mathbb{Z}/q$, $b \not\equiv 1 \pmod q$, we can solve $(a' + b \equiv 1 \pmod q)$, and the solution is unique.

Therefore,

$$f(c) = \sum_{\substack{b \bmod q \\ b \not\equiv 1 \pmod q}} \left(\frac{b}{q}\right).$$

We proved earlier that

$$\sum_{b \bmod q} \left(\frac{b}{q}\right) = 0$$

so

$$f(c) = \left(\frac{1}{q}\right) = -1,$$

when $c \not\equiv 0 \pmod{q}$.

Consequently

$$S_q^2 = (-1)^{\frac{q-1}{2}} \left[(q-1) + (-1) \sum_{\substack{c \bmod q \\ c \not\equiv 0 \bmod q}} \xi^c \right]$$

Claim: $\sum_{c \bmod q} \xi^c = 0$.

Proof of claim:

$$\sum_{c \bmod q} \xi^c = \sum_{(c-1) \bmod q} \xi^c = \sum_{c \bmod q} \xi^{c+1} = \xi \sum_{c \bmod q} \xi^c$$

$$\Rightarrow \underbrace{(1-\xi)}_{\neq 0} \sum_{c \bmod q} \xi^c = 0 \Rightarrow \sum_{c \bmod q} \xi^c = 0 \text{ as claimed.}$$

Proof 2 of claim:

$$\sum_{c \bmod q} \xi^c = 1 + \xi + \cdots + \xi^{q-1} = \frac{1-\xi^q}{1-\xi}$$

$$= 0 \text{ since } \xi^q = 1.$$

By claim,

$$S_q^2 = (-1)^{\frac{q-1}{2}} \left((q-1) + \underbrace{(-1)(0-1)}_{+1} \right)$$

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

This proves Lemma 1.

Lemma 1: $S_q^2 = (-1)^{\frac{q-1}{2}} q$

Lemma 2: $S_q^{p-1} \equiv (\frac{p}{q}) \pmod p$
(This happens in R mod p)

Proof of Lemma 2:

$$\begin{aligned} S_q^p &= \left(\sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^a \right)^p \\ &= \sum_{a \bmod q} \left(\frac{a}{q}\right)^p \xi^{ap} + pw, w \in R. \end{aligned}$$

$(\frac{a}{p})^q = (\frac{a}{p})$ because $(\frac{a}{q}) = \pm 1$ and p is odd

In other words,

$$S_q^p \equiv \sum_{a \bmod q} \left(\frac{a}{q}\right) \xi^{ap} \pmod p.$$

Since $p \neq q$, p is invertible mod q, and the map $a \mapsto ap$ is a permutation of $\mathbb{Z}/q$, also $ap \equiv 0 \pmod q$ iff $a \equiv 0 \pmod q$. so the sum over a mod q can be replaced with the sume over ap mod q. Write b for ap mod q. Then

$$a \equiv bp' \pmod q, \text{ where } pp' \equiv 1 \bmod q).$$

$$\Rightarrow S_q^p \equiv \sum_{b \bmod q} \left(\frac{bp'}{q}\right) \xi^b \pmod p \tag{*}$$

But

$$\left(\frac{bp'}{q}\right) = \left(\frac{b}{q}\right)\left(\frac{p'}{q}\right).$$

Since $p'p \equiv 1 \pmod q$,

$$\left(\frac{p'}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1 \Rightarrow \left(\frac{p'}{q}\right) = \left(\frac{p}{q}\right)$$

So

$$\left(\frac{bp'}{q}\right) = \left(\frac{b}{q}\right)\left(\frac{p}{q}\right).$$

So $(*)$ gives

$$S_q^p \equiv \left(\frac{p}{q}\right) \underbrace{\sum_{b \bmod q} \left(\frac{b}{q}\right) \xi^b}_{S_q} \pmod p$$

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

This is justified because

$$S_q \not\equiv 0 \pmod p,$$

which follows from lemma 1.

Proof of Theorem: Compute S^{p-1} in 2 different ways. On the one hand, by lemma 1,

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

$$\underset{\text{Euler}}{\equiv} \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \quad (\text{mod } p$$

$$\Rightarrow S^{p-1} \equiv \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{2}\right) \quad (\text{mod } p,$$

i.e.,

$$S^{p-1} \equiv (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \left(\frac{q}{p}\right) \pmod p.$$

On the other hand, by lemma 2,

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

So, putting them together we get

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

Last time, gave a proof of Quadratic Reciprocity law. More precisely we proved:

Theorem (Gauss) Let p, q be distinct, odd primes. Then

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

Example:

Check if 29 is a square mod 43: 29 and 43 are distinct odd primes, so by definition $29 \equiv \ (\text{mod } 43)$ iff $\left(\frac{29}{43}\right) = 1$. by QRL,

$$\begin{aligned}
\left(\frac{29}{43}\right) &= (-1)^{\frac{28(42)}{4}} \left(\frac{43}{29}\right) = \left(\frac{43}{29}\right) \\
&= \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) \\
\left(\frac{2}{29}\right) &= -1 \text{ as } 29 \equiv 5 \pmod 8 \\
\left(\frac{29}{43}\right) &= -\left(\frac{7}{29}\right)_{\text{QRL}} = -(-1)^{\frac{6(28)}{4}} \left(\frac{29}{7}\right) \\
&= -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1
\end{aligned}$$

So $29 \not\equiv \ (\text{mod } 43)$.

Remark: QRL tells you a way to know

1. whether q is a square mod p or not. But when it is a square, it gives no procedure to find the square root.

2. One can use QRL to check whether a number is a prime, similar to the way one uses Fermat's little theorem. For example, one can show that $m = 1729$ is not a prime by looking at

   $$y \stackrel{\text{def}}{\equiv} 11^{864} \pmod{1729}$$

   Note: $864 = \frac{1729-1}{2}$. So, if m is a prime, $y \equiv \left(\frac{11}{1729}\right) \pmod m$.

   Since $1729 \equiv 1 \pmod 4$, by QRL,

   $$\left(\frac{11}{1729}\right) = \left(\frac{1729}{11}\right) = \left(\frac{2}{11}\right) = -1$$

   as $11 \equiv 3 \pmod 8$. on the other hand, one can check using PARI, or by successively squaring mod $m = 1729$, that

   $$11^{864} \equiv 1 \pmod m.$$

(This is part of a homework problem.) Get a contradiction! So the only possibility is that 1729 is not a prime (which is easy to verify directly as $1729 = 13 \cdot 133 = 13 \cdot 7 \cdot 17$). But this method is helpful, when it works, for larger numbers.

A histoical remark: G.H.Hardy went to see Ramanujan, when the latter was dying of TB in England. Then Ramanujan asked Hardy if the number of the taxicab Hardy came in was an interesting number. Hardy said "No, not interesting, just 1729". Ramanujan replied immediately, saying, "On the contrary, the number *is* interesting because it is the first number which can be written as a sum of 2 cubes in two different ways". (Indeed we have

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

)

A second proof of quadratic recip. (Eisenstein) (Eisenstein's trignometric lemma)

Lemma: Let n be a positive, odd integer. Then

$$\frac{\sin nx}{\sin x} = (-4)^{\frac{n-1}{2}} \prod_{j=1}^{\frac{(n-1)}{2}} \left(\sin^2 x - \sin^2 \frac{2\pi j}{n}\right)$$

Proof: Up to us. Hint: treat as a polynomial in $\sin x$:

Example:

$n = 3$

$$\begin{aligned}
\text{LHS} &= \frac{\sin 3x}{\sin x} = \frac{\sin(2x+x)}{\sin x} \\
&= \frac{\sin 2x \cos x + \cos 2x \sin x}{\sin x} \\
&= \frac{2\sin x \cos^2 x + (1 - 2\sin^2 x)\sin x}{\sin x} \\
&= 2(1 - \sin^2 x) + (1 - 2\sin^2 x) = 3 - 4\sin^2 x \\
\text{RHS} &= -4(\sin^2 x - \left(\underbrace{\sin \frac{2\pi}{3}}_{\sqrt{3}/2}\right)^2 = -4\left(\sin^2 x - \frac{3}{4}\right) \\
&= 3 - 4\sin^2 x.
\end{aligned}$$

Sketch of proof of lemma: Use induction on n to show that

$$\frac{\sin nx}{\sin x} = f_n(\sin^2 x),$$

where f_n is a polynomial in $\sin^2 x$ of degree $\frac{n-1}{2}$.

$$(f_0(t) = 1,\ f_3(t) = 3 - 4t, \dots)$$

On the other hand, the RHS of lemma is also of the form $g_n(\sin^2 x)$, where g_n is the explicitly given polynomial in $\sin^2 x$ of degree $\frac{n-1}{2}$.

So it suffices to show that f_n and g_n have the same roots and that the leading coefficient of f_n is $(-4)^{\frac{n-1}{2}}$. So when we use induction on n, check that the leading coefficient is $(-4)^{\frac{(n-1)}{2}}$ and that its roots are

$$\left\{ \sin^2 \frac{2\pi j}{n} \middle| 1 \le j \le \frac{n-1}{2} \right\}.$$

Alternatively, check the constant coefficient by checking at $x \to 0$.

Recall Gauss' lemma:

$$\left(\frac{q}{p}\right) = \prod_{s \in S} e_s(q)$$

where $S = \{1, 2, \dots, \frac{p-1}{2}\}$ and $e_x(q) \in \{\pm 1\}$ defined by

$$qs = e_s(q)s',\ \text{with } s' \in S.$$

Applying $\sin(\frac{2\pi}{p})$, we get

$$\begin{aligned} \sin\left(\frac{2\pi qs}{p}\right) &= \sin\left(\frac{2\pi e_s(q)s'}{p}\right) \\ &= e_s(q)\sin\left(\frac{2\pi s'}{p}\right) \end{aligned}$$

since sin is an odd function. So

$$e_s(q) = \frac{\sin\left(\frac{2\pi qs}{p}\right)}{\sin\left(\frac{2\pi s'}{p}\right)}$$

By Gauss' lemma,

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{s\in S} \frac{\sin\left(\frac{2\pi q s}{p}\right)}{\sin\left(\frac{2\pi s'}{p}\right)} \\ &= \frac{\prod_{s\in S}\sin\left(\frac{2\pi q s}{p}\right)}{\prod_{s\in S}\sin\left(\frac{2\pi s'}{p}\right)}.\end{aligned}$$

Note the map $S \mapsto S'$ is a permutation of S. So,

$$\prod_{s\in S}\sin\left(\frac{2\pi s'}{p}\right) = \prod_{s\in S}\sin\left(\frac{2\pi s}{p}\right)$$

$$\Rightarrow \left(\frac{q}{p}\right) = \prod_{i=1}^{\frac{(p-1)}{2}} \frac{\left(\sin\frac{2\pi i q}{p}\right)}{\sin\frac{2\pi i}{p}} \tag{1}$$

Applying Eisenstein's trig. lemma with $n = q$ and sub. in (3), we get

$$\left(\frac{q}{p}\right) = (-4)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \prod_{i-1}^{\frac{(p-1)}{2}} \prod_{i-1}^{\frac{(q-1)}{2}} \left(\sin^2\left(\frac{2\pi i}{p}\right) - \sin^2\left(\frac{2\pi j}{p}\right)\right)$$

Can get everything we need from this without computing the sines:

Reversing the roles of p and q, we get

$$\left(\frac{p}{q}\right) = (-4)^{\frac{q-1}{2}} \prod_{i-1}^{\frac{p-1}{2}} \prod_{i-1}^{\frac{q-1}{2}} \left(\sin^2\left(\frac{2\pi j}{p}\right) - \sin^2\left(\frac{2\pi i}{p}\right)\right)$$

Comparing (3) and (4), we see that

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