MATH 575 - Project

Connor Davis, Youssef Katamish, Nicholas VanderLaan

August 16, 2017

In this final project we will explore the relation between a problem we discussed in class, namely:

For what rational primes p is 7 a cube mod p?

and the Langlands program. When working on this project, you will at various points have to take on faith something said below. Also, don't be afraid to make educated guesses. (If you don't know the definition of something below, feel free to come by and ask me.)

1. First, recall our discussion in class, and write out a criterion for 7 to be a cube mod p in terms of the splitting of p in the field $\mathbb{Q}(\omega)$ using cubic reciprocity. (When $p \equiv 1 \bmod 3$, this should depend on the congruence class of π (or $\bar{\pi}$) mod 7, where $p = \pi\bar{\pi}$ is the decomposition of p as a product of primary primes.) Use this to determine the set of primes less than 150 for which 7 is a cube mod p.

   Proof. We consider two cases:

   First the case where $p \equiv 1(3)$: 7 splits in $\mathbb{Z}[\omega]$, hereby referred to as D as the product of $(2+3\omega)(-1-3\omega) = \lambda\overline{\lambda}$. Additionally, because $p \equiv 1(3)$, $p = \pi\overline{\pi}$ where $\pi \in D$, and $\overline{\pi}$ is the conjugate of π. We can assume π is primary, else we can just split 7 differently in D. The conjugates of primary primes are primary $\implies$ $\overline{\pi}$ is also primary. Then $\chi_\pi(7) = \chi_\pi(\lambda\bar{\lambda}) = \chi_\pi(\lambda)\chi_\pi(\bar{\lambda})$. By cubic reciprocity, we have that $\chi_\lambda(\pi)\chi_{\overline{\lambda}}(\pi)$. $\chi_\pi(7) = 1$ is true then when either $\chi_\lambda(\pi) = \chi_{\overline{\lambda}}(\pi) = 1$ or $\chi_\lambda(\pi) = \omega, \chi_{\overline{\lambda}}(\pi) = \omega^2$, or $\chi_\lambda(\pi) = \omega^2, \chi_{\overline{\lambda}}(\pi) = \omega \bowtie$.

   $\chi_\lambda(\pi) = \pi^{\frac{N(\lambda)-1}{3}}(\lambda) = \pi^2(\lambda)$. We can view equivalence classes mod λ as classes in $\mathbb{Z}/N(\lambda)\mathbb{Z}$ by the natural isomorphism. So

π	$\pi^2(\lambda)$	π	$\pi^2(\overline{\lambda})$
1	1	1	1
2	ω	2	ω^2
3	ω^2	3	ω
4	ω^2	4	ω
5	ω	5	ω^2
6	1	6	1

   Thus we need to simultaneously satisfy the congruences given in $\bowtie$. By the Chinese remainder theorem, we get the following:

factor	(π, λ)
$4+\omega$	$(1,-1)$
$3+6\omega$	$(-1,1)$
$1+\omega$	$(2,-2)$
$6+5\omega$	$(-2,2)$
$5+3\omega$	$(3,-3)$
$2+4\omega$	$(-3,3)$

Second the case where $p \equiv 2(3)$: Here we recall that the map

$$\begin{aligned} f : \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ x &\mapsto x^3 \end{aligned}$$

is an isomorphism, so 7 will always be congruent to a cube mod p.

Of the set of primes less than 150: $\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47\}$ $\cup\{53,59,61,67,71,73,79,83,89,97,101,103,107,109,113,127,131,137,139,149\}$, $A := \{2,5,11,17,23,41,47,53,59,71,83,89,101,107,113,127,139,149\}$ are congruent to $2 \mod (3) \implies 7$ is a cube mod $p \in A$. Of the remaining primes, 7 is congruent to a cube only for $\{19,73\}$.

□

2. Let q be a power of a prime p and let $\mathbb{F}_{q^n}$ denote the finite field with q^n elements. Show that $\bar{\sigma}(x) = x^q$ is a field automorphism of $\mathbb{F}_{q^n}$ that acts as the identity on $\mathbb{F}_q$. This is called the Frobenius automorphism. The set of automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is naturally a group, called the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Show that this group has n elements and in fact is cyclic of order n generated by $\bar{\sigma}$.

Proof. We will first show that $\bar{\sigma}(x) = x^q$ is a field homomorphism. i.e. we need to show that $\bar{\sigma}(0) = 0$, $\bar{\sigma}(a+b) = \bar{\sigma}(a) + \bar{\sigma}(b)$, $\bar{\sigma}(ab) = \bar{\sigma}(a)\bar{\sigma}(b)$.

The first equality is trivial.

Note that the characteristic of the field is p (since q is a power of p, i.e. $q = p^k$ for some $k \in \mathbb{Z}^+$). Hence, we have that $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{F}_{q^n}$. A simple inductive argument shows that $(a+b)^{p^x} = a^{p^x} + b^{p^x}$ for all $a, b \in \mathbb{F}_{q^n}$ and $x \in \mathbb{Z}^+$. Thus, we have that $\bar{\sigma}(a+b) = (a+b)^q = (a+b)^{p^k} = a^{p^k} + b^{p^k} = a^q + b^q = \bar{\sigma}(a) + \bar{\sigma}(b)$ for all $a, b \in \mathbb{F}^{q^n}$

We have that $\bar{\sigma}(ab) = (ab)^q = a^q b^q = \bar{\sigma}(a)\bar{\sigma}(b)$ for all $a, b \in \mathbb{F}^{q^n}$, since $\mathbb{F}_{q^n}$ is a field and hence multiplication is commutative.

We will now show that $\bar{\sigma}$ is a field automorphism. It suffices to show that $\bar{\sigma}$ is injective, since $\bar{\sigma}$ is a field endomorphism to a finite field. Note that $\ker\bar{\sigma}$ is an ideal in $\mathbb{F}_{q^n}$, meaning that $\ker\bar{\sigma}$ is trivial or $\mathbb{F}_{q^n}$. Since $\bar{\sigma}$ is a field endomorphism, $\ker\bar{\sigma} = \mathbb{F}_{q^n}$ iff $\ker\bar{\sigma} = 0$. Since $\bar{\sigma}(1) = 1$, $\bar{\sigma} \neq 0$ and hence $\ker\bar{\sigma} = 0$. Thus, $\bar{\sigma}$ is injective.

Hence, $\bar{\sigma}$ is a field automorphism.

We will now show that $\bar{\sigma}$ acts as the identity of $\mathbb{F}_q$. Let $x \in \mathbb{F}_q$. If $x = 0$, then $\bar{\sigma}(x) = 0^q = 0$. If $x \neq 0$, then $x \in \mathbb{F}_q^\times$ and hence $x^{q-1} = 1$. Thus, this means that $x^q = x$ and hence $\bar{\sigma}(x) = x$, as required.

Let $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ represent the group of the set of all automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We will show that this group is a cyclic group of order n.

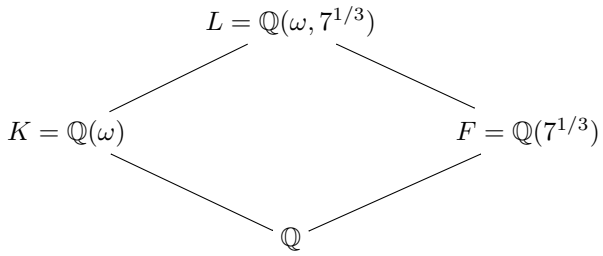
We will first prove a more general statement. We will prove that if L/K be a finite extension of finite fields, where $[L:K] = n$, then $|\mathrm{Gal}(L/K)| \leq n$. Since L is a finite field, then L is generated by an element $\alpha \in L$. First note that $\alpha \notin K$ and hence α is the root of an irreducible polynomial $p(x) \in K[x]$ such that the degree of p is n. Thus, we have that any automorphism must map α to a root of p. Since p can have at most n roots in L, we have that there are at most n different automorphisms on L that fix K.

We will now show that $\bar{\sigma}^k$ is distinct for all $k \in \{1, \ldots, n-1\}$. Recall that $\mathbb{F}_{q^n}^\times$ is cyclic of order $q^n - 1$. Let α be the generator of $\mathbb{F}_{q^n}$. We have that: $1, \alpha^q \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ are all distinct elements. Hence, this means that $\bar{\sigma}(\alpha), \bar{\sigma}^2(\alpha), \ldots, \bar{\sigma}^{n-1}(\alpha)$ are all distinct. Hence, we have that $\bar{\sigma}^k$ are distinct for all $k \in \{1, \ldots, n-1\}$.

Since $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ and since $\bar{\sigma}^k$ is distinct for $k \in \{0, \ldots, n-1\}$, we have that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n that is generated by $\bar{\sigma}$.

□

3. Consider the diagram of fields:



Then $G = \mathrm{Gal}(L/\mathbb{Q})$, which as above is defined to be the group of automorphisms of $L/\mathbb{Q}$, is a group of order 6 generated by σ and τ, where

$$\begin{aligned} \sigma(\omega) = \omega^2, \quad \sigma(7^{1/3}) = 7^{1/3} \\ \tau(\omega) = \omega, \quad \tau(7^{1/3}) = \omega \cdot 7^{1/3}. \end{aligned}$$

Show that G is isomorphic to S_3. Write down all the different conjugacy classes in G.

Proof. Recall from group theory that there are only two groups of order 6 up to isomorphism. The two groups are: $\mathbb{Z}/6\mathbb{Z}$ and S_3. Note that $\mathbb{Z}/6\mathbb{Z}$ is an abelian group and S_3 is a non-abelian group.

Hence, to show that G is isomorphic to S_3, it suffices to show that G is not abelian.

Let $7^{1/3} \in L$ and consider $\sigma \circ \tau$ and $\tau \circ \sigma$. We have that:

$$(\sigma \circ \tau)(7^{1/3}) = \sigma(\tau(7^{1/3})) = \sigma(\omega \cdot 7^{1/3}) = \omega^2 \circ 7^{1/3}$$

and

$$(\tau \circ \sigma)(7^{1/3}) = \tau(\sigma(7^{1/3})) = \tau(7^{1/3}) = \omega \cdot 7^{1/3}$$

Hence, this means that $\tau \circ \sigma \neq \sigma \circ \tau$ and hence G is not abelian. Since G is a group of order 6, G is isomorphic to S_3, as required.

Recall that two elements $a, b \in G$ are *conjugates* if there exists $g \in G$ such that $g^{-1}ag = b$. From group theory, we know that conjugacy is an equivalence relation and hence the partitions are called the *conjugacy classes*.

To compute the conjugacy classes of G, we will first write G in terms of the generators σ and τ.

For notational purposes, from this point on, we will write $\sigma\tau$ to denote $\sigma \circ \tau$.

We have that $\sigma\tau \neq \tau\sigma$, hence those are two other distinct elements.

Note that $\sigma^2 = \mathrm{Id}$, and $\tau^2 \neq \mathrm{Id}$ yet $\tau^3 = \mathrm{Id}$ and hence $G = \{1, \sigma, \tau, \tau^2, \sigma\tau, \tau\sigma\}$.

Before we proceed, we will compute a relation that will aid with the computation throughout this problem. Note that $\sigma\tau^2(\omega) = \sigma(\omega) = \omega^2$ and $\sigma\tau^2(7^{1/3}) = \sigma(\tau(\omega \cdot 7^{1/3}) = \sigma(\omega^2 \cdot 7^{1/3}) = \omega \cdot 7^{1/3}$. Observe that $\tau\sigma(\omega) = \tau(\omega^2) = \omega^2$ and $\tau\sigma(7^{1/3}) = \tau(7^{1/3}) = \omega \cdot 7^{1/3}$. Hence, we have that $\tau\sigma = \sigma\tau^2$.

Let C_x denote the conjugacy class of $x \in G$.

Clearly, 1 is in a conjugacy class by itself (since $g \in G$ implies that $g^{-1} \cdot 1 \cdot g = g^{-1}g = 1$). Hence, we have that $C_1 = \{1\}$

We will first compute the conjugacy class of σ. Note that $\tau^{-1} = \tau^2$ and hence $\tau^2\sigma\tau = \tau(\tau\sigma)\tau = \tau(\sigma\tau^2)\tau = \tau\sigma$. Hence, this means that $\sigma, \tau\sigma \in C_\sigma$. Similarly, $\tau\sigma\tau^2 = (\tau\sigma)\tau^2 = (\sigma\tau^2)\tau^2 = \sigma\tau$ and hence $\sigma\tau \in C_\sigma$. Consider $(\tau\sigma)^{-1} = \sigma\tau^2$, we have that $\sigma\tau^2\sigma\tau\sigma = (\sigma\tau^2)\sigma\tau\sigma = (\tau\sigma)\sigma\tau\sigma = \tau^2\sigma = \tau\sigma\tau^2 = \sigma\tau$. Finally, $(\sigma\tau)^{-1} = \tau^2\sigma$ and hence $\tau^2\sigma\sigma\sigma\tau = \tau^2\sigma\tau = \tau\sigma$. Thus, we have that $C_\sigma = \{\sigma, \sigma\tau, \tau\sigma\}$.

Finally, consider C_τ. We have that $\sigma\tau\sigma = \sigma\sigma\tau^2 = \tau^2$ and hence $\tau^2 \in C_\tau$. Thus, since the conjugacy classes partition G, we have that $C_1 = \{1\}, C_\sigma = \{\sigma, \tau\sigma, \sigma\tau\}$ and $C_\tau = \{\tau, \tau^2\}$ are the conjugacy classes of G.

□

4. Let R_L denote the ring of integers of L. Let $\mathfrak{p}$ be a (non-zero) prime ideal in R_L. Then $\mathfrak{p} \cap \mathbb{Z} = (p)$ is a prime ideal in $\mathbb{Z}$ and we get an extension of finite fields

$$\begin{array}{c} R_L/\mathfrak{p} = \mathbb{F}_{\mathfrak{p}} \\ | \\ \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \end{array}$$

Note that G acts naturally on R_L and any element of G sends a prime ideal in R_L to a prime ideal. (Why?) Let $D_{\mathfrak{p}}$ denote the subgroup of G given by

$$D_{\mathfrak{p}} = \{\theta \in G : \ \theta(\mathfrak{p}) = \mathfrak{p}\}.$$

Then there is a natural map

$$D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p).$$

(Why?) FACT: This map is always surjective and if $p \neq 3, 7$, then this map is an isomorphism. In particular, in this case, we get a canonical element in G attached to $\mathfrak{p}$ called $\mathrm{Frob}_{\mathfrak{p}}$ or the Frobenius at $\mathfrak{p}$, namely the one that corresponds to the (Frobenius) generator of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ defined in Problem 2.

Proof. We show that G acts as an automorphism on R_L. Fix $g \in G$ and $\alpha \in R_L$. Since $g \in G$, we have that $g(x+y) = g(x) + g(y)$ and that g fixes the elements of $\mathbb{Q}$.

(a) $g(\alpha) \in R_L$

α is the root of a polynomial with integer coefficients:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$$

To show that $g(\alpha)$ is also in R_L, we see that

$$\begin{aligned} g(0) &= g(\alpha^n + a_{n-1}\alpha^{n-1} \ldots + a_0) \\ &= g(\alpha^n) + g(a_{n-1}\alpha^{n-1} + \ldots + g(a_0) \\ &= g(\alpha)^n + a_{n-1}\alpha^{n-1} + \ldots + g(a_0) \end{aligned}$$

Note that since $0, a_0 \in \mathbb{Z}, g(0) = 0$, so we have that $g(\alpha)$ is the root to a polynomial with integer coefficients, and is thus an algebraic integer.

(b) g is surjective over R_L.

We want to show $\exists \beta \in R_L$ such that $g(\beta) = \alpha$. We know that $\exists \gamma \in L$ such that $g(\gamma) = \alpha$ since g is an automorphism over L. Since $g(\gamma) = \alpha$, we have that

$$g(\gamma)^n + a_{n-1}g(\gamma)^{n-1} + \ldots + a_1 g(\gamma) + a_0 = 0$$

or, equivalently,

$$g(\gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma) + a_0 = 0$$

We want to show that γ is itself an algebraic integer, meaning that γ is the root to a polynomial with integer coefficients. We continue, noting that $g^{-1}(a_0) = a_0$

$$\begin{aligned} g(\gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma) &= -a_0 \\ g^{-1}g(\gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma) &= -g^{-1}(a_0) \\ \gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma &= -a_0 \\ \gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_1\gamma + a_0 &= 0 \end{aligned}$$

as desired.

This shows that g is an automorphism on R_L, since injectivity comes for free: any injective map is injective when restricted. Thus G acts naturally on R_L insofar as it is the group of automorphisms of R_L.

Next, we show that for a prime ideal $\mathfrak{p}$ in $R_L, g(\mathfrak{p})$ is also a prime ideal. First we show that $g(\mathfrak{p})$ is an ideal. We show it is closed under addition and multiplication.

(a) $a, b \in g(\mathfrak{p}), a + b \in g(\mathfrak{p})$

Well, $a, b \in g(\mathfrak{p}) \implies \exists c, d \in \mathfrak{p}$ such that $g(c) = a, g(d) = b$ Then, $\mathfrak{p}$ is an ideal so $c + d \in \mathfrak{p}$, meaning $g(c + d) = g(c) + g(d) = a + b \in g(\mathfrak{p})$

(b) $a \in g(\mathfrak{p}), r \in \mathbb{R}_L$

We proceed similarly. $a \in g(\mathfrak{p}) \implies \exists c \in \mathfrak{p}$ such that $g(c) = a$. Since $\mathfrak{p}$ is an ideal, $rc \in \mathfrak{p}$. Thus $g(rc) = rg(c) = ra \in g(\mathfrak{p})$

Thus $g(\mathfrak{p})$ is an ideal.

Next we show it is, in fact, a prime ideal. By definition, $g(\mathfrak{p})$ will be a a prime ideal if for $ab \in g(\mathfrak{p})$, either $a \in g(\mathfrak{p})$ or $b \in g(\mathfrak{p})$. So, fix $ab \in g(\mathfrak{p})$ and assume that $a \notin g(\mathfrak{p})$. Since $ab \in g(\mathfrak{p}), \exists x \in \mathfrak{p}$ such that $g(x) = ab$. But since $a \notin g(\mathfrak{p}), \forall y \in \mathfrak{p}, g(y) \neq a$. We want to show that there exists an $z \in \mathfrak{p}$ such that $g(z) = b$. Well, $\mathfrak{p}$ is a prime ideal and $g^{-1}(ab) = g^{-1}(a)g^{-1}(b) \in \mathfrak{p}$. If $g^{-1}(a)$ were in $\mathfrak{p}$, then we contradict that $a \notin g(\mathfrak{p})$. So $g^{-1}(b) \in \mathfrak{p}$, which implies that $b \in g(\mathfrak{p})$.

Thus $g(\mathfrak{p})$ is a prime ideal.

Given that elements of G map prime ideals in R_L to prime ideals, we can consider those maps of G that map a particular prime ideal $\mathfrak{p}$ to itself. Let

$$D_{\mathfrak{p}} = \{\theta \in G : \theta(\mathfrak{p}) = \mathfrak{p}\}$$

We show there exists a natural map $\phi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$. $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/F_p)$ is the group of automorphisms on $\mathbb{F}_{\mathfrak{p}}$ that fix $\mathbb{F}_p$

Consider the map that sends $\theta([\alpha]) \mapsto [\theta(\alpha)]$. First we show ϕ maps into $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$. To do this we show ϕ maps the identity to the identity, and that the resultant automorphisms are in fact automorphisms. That is, they are additive, multiplicative, surjective, and injective. Fix $\theta \in D_{\mathfrak{p}}$.

(a) identity to identity:

$$\begin{aligned} \phi(\theta([1])) &= [\theta(1)] \\ &= [1] \qquad\qquad \text{as } \theta \text{ is an automorphism} \end{aligned}$$

(b) Additive:

$$\begin{aligned}[\theta(\alpha)+\theta(\beta)] &= \phi(\theta([\alpha])+\theta[\beta]) \\ &= \phi(\theta([\alpha]))+\phi(\theta([\beta])) \\ &= [\theta(\alpha)]+[\theta(\beta)]\end{aligned}$$

(c) Multiplicative:

$$\begin{aligned}[\theta(r\cdot\alpha)] &= \phi(\theta([r\cdot\alpha]) \\ &= r\cdot\phi(\theta[\alpha]) \\ &= r\cdot[\theta(\alpha)]\end{aligned}$$

(d) Injective: Assume that $[\theta(\alpha)] = [\theta(\beta)]$. We have

$$\begin{aligned}0 &= [\theta(\alpha)]-[\theta(\beta)] && \text{hypothesis} \\ &= [\theta(\alpha)-\theta(\beta)] && \text{additivity} \\ &= [\theta(\alpha-\beta)] && \text{additivity of } \theta\end{aligned}$$

So, $\alpha = \beta$. Thus $[\theta(x)]$ is injective.

(e) Surjective: Follows from injectivity and the fact that $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is a finite set.

And note that these automorphisms are well defined since $\theta \in D_{\mathfrak{p}}$ fix $\mathfrak{p}$ and as $\theta \in G$, they send algebraic integers to algebraic integers.

Next, we show that ϕ is a homomorphism. We see that ϕ takes the identity automorphism to the identity automorphism in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p$: Fix some $\alpha \in R_L$, so that $[\alpha]$ is a conjugacy class in $\mathbb{F}_{\mathfrak{p}}$. We have

$$\begin{aligned}\phi(e[\alpha]) &= [e(\alpha)] \\ &= [\alpha]\end{aligned}$$

Recall that $G = \mathrm{Gal}(L/\mathbb{Q})$. If $\theta \in D_{\mathfrak{p}} \subset G$, then $\theta(\mathfrak{p}) = \mathfrak{p}$. Hence, θ maps a specific prime ideal to itself.

The natural map $\phi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ can be given by $\phi(\theta) = \theta|_{\mathbb{F}_{\mathfrak{p}}}$.

Note that $\theta|_{\mathbb{F}_{\mathfrak{p}}}$ is constant over $\mathbb{F}_p$, as $\mathbb{F}_p \subset \mathbb{Q}$ and $\theta \in \mathrm{Gal}(L/\mathbb{Q})$.

To show that ϕ is a homomorphism, we will show that ϕ respects group operations:

$$\begin{aligned}\phi(\theta_1\theta_2) &= \\ &= (\theta_1\theta_2)|_{\mathbb{F}_{\mathfrak{p}}} \\ &= (\theta_1)|_{\mathbb{F}_{\mathfrak{p}}} + (\theta_2)|_{\mathbb{F}_{\mathfrak{p}}} \\ &= \phi(\theta_1)\phi(\theta_2)\end{aligned}$$

as required.

□

5. Given any prime p in $\mathbb{Z}$, there exists a prime $\mathfrak{p}$ in R_L such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Then one gets an element $\text{Frob}_\mathfrak{p}$ above which may very well depend on the choice of $\mathfrak{p}$ above (p). However, the *conjugacy class* of $\text{Frob}_\mathfrak{p}$ in G only depends on p !! This gives a conjugacy class in G called Frob_p. How does Frob_p depend on the congruence class of p mod 3? (Make an educated guess based on your knowledge of the cubic residue symbol and justify it as much as possible.)

   We have two cases, $p \equiv 1(3), p \equiv 2(3)$. We deal with the former first. Fix $p \equiv 1(3)$. Set $\alpha = \sqrt[3]{7}$. Let $\mathfrak{p}$ be a prime ideal in R_L such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Recall that the Frobenius automorphism $\sigma(x) = x^p$, so $\sigma(\alpha) = \alpha^p$. We compute

$$\sigma(\omega) = \omega^p \equiv \omega$$

   But this is ambiguous, since it does not tell us if σ corresponds to a class that is the identity, or that of a rotation. Thus we proceed further. Since $p \equiv 1(3)$, we know that when $p \equiv 1(3)$, p splits into π and $\overline{\pi}$ over the Eisenstein integers, meaning $\pi, \overline{\pi}$ live in $\mathbb{Q}[\omega]$. Without loss of generality, assume that π is primary. Also, we recall our definition of the cubic reciprocity symbol. We have that

$$\left(\frac{x}{y}\right) = x^{\frac{Ny-1}{3}} \mod y$$

   Thus, since $N\pi = p$,

$$\left(\frac{7}{\pi}\right) = 7^{\frac{p-1}{3}} \mod \pi = \alpha^{p-1} \mod \pi$$

   Multiplying by α on both sides, we have that

$$\left(\frac{7}{\pi}\right)\alpha = \alpha^p \mod \mathfrak{p} = \sigma(\alpha)$$

   where we are modulo $\mathfrak{p}$ not π since $\alpha \in R_L \backslash R_K$. Then, the most right hand side is the Frob_p. We see that the LHS has two terms, α and the cubic reciprocity symbol which evaluates to either $\{1, \omega, \omega^2\}$, each of which is in its own conjugacy class. Then since multiplying by α does not change the conjugacy class of either $1, \omega, \omega^2$, and the LHS depends only on p (based on p's splitting into π), then

$$\sigma(\alpha) = \begin{cases} \alpha, \text{ if } \left(\frac{7}{\pi}\right) = 1 \\ \alpha\omega, \text{ if } \left(\frac{7}{\pi}\right) = \omega \\ \alpha\omega^2, \text{ if } = \left(\frac{7}{\pi}\right) = \omega^2 \end{cases}$$

   Recalling that $\sigma(\omega) = \omega$, if we are in the first case that $\sigma(\alpha) = \alpha$, then we have that Frob_p is the identity, and is therefore in such a conjugacy class. In the other two cases, it corresponds to a rotation element, and is therefore in such a conjugacy class.

   Next, we consider $p \equiv 2(3)$ This is very simple as $\sigma(\omega) \equiv \omega^p = \omega^2$. Thus the Frob_p is a reflection conjugacy class.

6. One way to understand a group is through its representations. A representation of a group G on a complex vector space V is a homomorphism

$$G \to \mathrm{GL}(V) = \mathrm{Aut}(V),$$

where $\mathrm{Aut}(V)$ denotes the (linear) automorphisms of V. Thus a representation may be viewed as giving an action of G on V, in which each element of G acts as a linear operator on V. If V has dimension n, and you pick a basis for V, then this may be viewed as a homomorphism

$$G \to \mathrm{GL}_n(\mathbb{C}),$$

which is called the associated matrix representation. A representation is called irreducible if there does not exists a non-zero proper subspace W of V which is preserved by all the elements of G. The group $G \simeq S_3$ has exactly 3 irreducible representations (up to isomorphism). These are:

- The (one dimensional) *trivial* representation. What do you think this is?
- The (one dimensional) *sign* representation. What do you think this is?
- A two dimensional representation ρ which we shall call the *standard representation*. This representation is obtained by thinking of S_3 as the group of symmetries of an equilateral triangle with center at the origin in $\mathbb{R}^2$, and representing the elements of S_3 as 2×2 matrices with real coefficients. Write down this matrix representation explicitly. The actual matrices you get will depend on the choice of basis for $\mathbb{R}^2$ you pick, but the traces will be independent of choice of basis. For each element θ in G, write down $\mathrm{tr}(\rho(\theta))$ as well as the (possibly complex) eigenvalues of $\rho(\theta)$. Notice that θ is constant on conjugacy classes. (Note that this representation lands in $\mathrm{GL}_2(\mathbb{R})$ but we can think of it as landing in $\mathrm{GL}_2(\mathbb{C})$, so we also get a two dimensional complex representation.)

Proof. Let $G \simeq S_3$.

- The (one-dimensional) *trivial* representation, from the name, is the representation $\phi : G \to \mathrm{GL}_1(\mathbb{C})$ that maps every element in G to 1 (where 1 is the 1-dimensional matrix [1]).

  Clearly ϕ is a homomorphism, since $\phi(ab) = 1 = 1 \cdot 1 = \phi(a)\phi(b)$. The reason why ϕ maps to 1 as opposed to 0 is because $0 \notin \mathrm{GL}_1(\mathbb{C})$.
- Recall that S_3 is the symmetric group of order 3. i.e. the elements of the group are permutations of the set of 3 elements. The (one-dimensional) *sign* representation, from the name, would be the homomorphism that maps a permutation to its *sign*, denote this representation by ϕ. The sign of a permutation is either even or odd and hence $\phi : G \to \{1, -1\}$, where $\phi(g) = 1$ if the sign of g is an even permutation and $\phi(g) = -1$ if g is an odd permutation.

  We will show that ϕ is a homomorphism. Suppose that $a, b \in G$. If both a and b are even permutations, then $\phi(ab) = 1 = 1 \cdot 1 = \phi(a)\phi(b)$. If one of a or b is an odd permutation, without loss of generality, assume a is an odd permutation and b is an even permutation, ab is an odd permutation; hence, $\phi(ab) = -1 = (-1) \cdot 1 = \phi(a)\phi(b)$. Finally, if both a and b are odd permutations, then ab is an even permutation; thus, $\phi(ab) = 1 = (-1) \cdot (-1) = \phi(a)\phi(b)$.
- As suggested, we will think of S_3 as the dihedral group of order 6 (which we will denote as D_6. The group D_6 is the group of all isometries of the regular triangle centered at

$(0,0)$. The isometries of the equilateral triangle are: rotation of $\pi/3$, reflection about the y-axis, and any composition of the aforementioned isometries.

Recall (from problem 3) that $G = \{1, \sigma, \tau, \tau^2, \sigma\tau, \sigma\tau^2\}$ where $\sigma\tau^2 = \tau\sigma$.

Since the dihedral group has symmetries of rotation (by $\pi/3$) and reflection (about the y axis). It would seem that τ denotes the rotation, since $\tau^2 \neq 1$ yet $\tau^3 = 1$ and that σ denotes the reflection, since $\sigma^2 = 1$.

Thus, we will define ρ by:

$$\rho(\tau) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

and

$$\rho(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

By defining ρ on τ and σ, ρ is forced to be a homomorphism. We verify this explicitly:

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho(\tau) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$\rho(\tau^2) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \rho(\tau)\rho(\tau)$$

$$\rho(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho(\sigma\tau) = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \rho(\sigma)\rho(\tau)$$

$$\rho(\tau\sigma) = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \rho(\tau)\rho(\sigma)$$

We can compute the trace and eigenvalues of each of the representations:

x	$\rho(x)$	$\mathrm{tr}(\rho(x))$	eigenvalues
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	2	$1, 1$
τ	$\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$	-1	$-\frac{1}{2} - \frac{i\sqrt{3}}{2}, -\frac{1}{2} + \frac{i\sqrt{3}}{2} (= \omega, \omega^2)$
τ^2	$\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$	-1	$-\frac{1}{2} - \frac{i\sqrt{3}}{2}, -\frac{1}{2} + \frac{i\sqrt{3}}{2} (= \omega, \omega^2)$
σ	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	0	$-1, 1$
$\sigma\tau$	$\begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$	0	$-1, 1$
$\tau\sigma$	$\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$	0	$-1, 1$

Recall that the conjugacy classes of G are $C_1 = \{1\}, C_\tau = \{\tau, \tau^2\}, C_\sigma = \{\sigma, \sigma\tau, \tau\sigma\}$. Note that if $\theta \in C_1$, then $\mathrm{tr}(\rho(\theta)) = 1$, if $\theta \in C_\tau$, then $\mathrm{tr}(\rho(\theta) = -1$, and if $\theta \in C_\sigma$, then $\mathrm{tr}(\rho(\theta)) = 0$. Hence, we can conclude that $\mathrm{tr}(\rho)$ is constant on the conjugacy class. Also note that elements in the same conjugacy class have the same eigenvalues.

□

7. The Langlands program tells us how to formulate a non-abelian reciprocity law in this context. Namely the conjugacy classes Frob_p in G are related in the following way:

> *There exists an integer N and a modular form f of weight one for $\Gamma_1(N)$ such that for all but finitely many p, the pth Fourier coefficient of f equals $\mathrm{tr}(\rho(\mathrm{Frob}_p))$.*

In this problem we will learn what this statement approximately means and find the form f.

The group $\Gamma_1(N)$ is given by

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z});\ c \equiv 0 \bmod N,\ a \equiv d \equiv 1 \bmod N \right\}.$$

Check that this is a group.

Proof. Closure: Let

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in \Gamma_1(N).$$

Then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

$c, g \equiv 0(N) \implies ce + dg \equiv 0(N)$. $a, e \equiv 1(N)$ and $g \equiv 0(N) \implies bg \equiv 0(N) \implies ae + bg \equiv 1(N)$. Similarly, $d, h \equiv 1(N)$ and $c \equiv 0(N)$ so $cf \equiv 0(N) \implies cf + dh \equiv 1(N)$. Thus we have closure under multiplication.

Identity: The Id matrix will do. Let

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N).$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

All that remains is to show $\mathrm{Id} \in \Gamma_1(N)$. This is clear because $0 \equiv 0(N), 1 \equiv 1(N)$.

Inverse: Again, let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N).$$

Inversion is done in the standard way,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

In fact, since $A \in SL_2(\mathbb{Z})$, we have $1/(ad - bc) = 1$ since this is the reciprocal of the determinant. Thus

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

We check $A^{-1} \in \Gamma_1(N)$: $d \equiv a \equiv 1(N)$, $c \equiv -c \equiv 0(N)$, and $\det(A^{-1} = 1 \cdot \det(A) = 1 \implies A^{-1} \in SL_2(\mathbb{Z})$.

$$AA^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad-bc & cd-dc \\ -ba+ba & -bc+da \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & -bc+da \end{bmatrix}.$$

Further, $ad - bc = -bc + da = \det(A) = 1 \implies AA^{-1} = \mathrm{Id}$.

$$A^{-1}A = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} da - bc & db - bd \\ -ca + ac & -cb + ad \end{bmatrix} = \begin{bmatrix} da - bc & 0 \\ 0 & -cb + ad \end{bmatrix}.$$

We note that $\det(A^{-1}) = da - bc = 1 \implies A^{-1}A = \mathrm{Id}$. Note multiplication and addition are well behaved (Communitive) in $\mathbb{Z}$ making this possible.

Associativity: This follows from the fact that matrix multiplication is associative, but here goes: Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, E = \begin{bmatrix} e & f \\ g & h \end{bmatrix}, J = \begin{bmatrix} j & k \\ l & m \end{bmatrix} \in \Gamma_1(N).$$

We need to show

$$\begin{gathered} A(EJ) \stackrel{?}{=} (AE)J \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} j & k \\ l & m \end{bmatrix} \right) \stackrel{?}{=} \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} j & k \\ l & m \end{bmatrix} \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} ej + fl & ek + fm \\ gj + hl & gk + hm \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \begin{bmatrix} j & k \\ l & m \end{bmatrix} \\ \begin{bmatrix} aej + afl + bgj + bhl & aek + afm + bgk + bhm \\ cej + cfl + dgj + dhl & cek + cfm + dgk + dhm \end{bmatrix} = \begin{bmatrix} aej + bgj + afl + bhl & aek + bgk + afm + bhm \\ cej + dgj + cfl + dhl & cek + dgk + cfm + dhm \end{bmatrix} \end{gathered}$$

Thus $\Gamma_1(N)$ a group.

□

A modular form of weight one for $\Gamma_1(N)$ is an analytic function $f : \mathbf{H} \to \mathbb{C}$, where

$$\mathbf{H} = \{z \in \mathbb{C} : \ \mathrm{Im}(z) > 0\},$$

that satisfies

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)f(z)$$

for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N)$. Show that f is forced to satisfy

$$f(z + 1) = f(z).$$

Proof. For f(z+1) we have that $a = 1, b = 1, c = 0, d = 1$ meaning, which means $cz + d \equiv 1$, so

$$\begin{aligned} f(z + 1) &= f\left(\frac{z + 1}{cz + d}\right) \\ &= f(z + 1) \\ &= (cz + d)f(z) = f(z) \end{aligned}$$

□

This periodicity implies that f has a *Fourier expansion* or q-expansion in the variable $q = e^{2\pi iz}$:

$$f(z) = \sum_{n=1}^{\infty} a_n q^n.$$

Then Langlands conjectures (which are known in this particular case) predict that there is such an f satisfying:

$$a_p = \mathrm{tr}\rho(\mathrm{Frob}_p) \tag{1}$$

for all rational primes $p \neq 3, 7$ and for a precise value of N. We will now try to find this form in the tables of weight one forms at the following website:

http://people.maths.ox.ac.uk/lauder/weight1/

You will want to look in one of the first 10 tables. The *level* N that you are looking for should be of the form $3^r 7^s$ for some small integers r and s. Once you have found your form and hence N, compare the a_p of the form f with your answer to Question 1. Check that equation (1) holds for all rational primes less than 150.

(If you don't understand the content of the tables at the website above, feel free to stop by my office.)

Explain why knowing the modular form f completely solves the problem of finding the rational primes p such that 7 is a cube mod p.

At $N = 1323$, we have the polynomial

$$\begin{aligned} f := {} & q + q^4 - q^{13} + q^{16} + 2q^{19} + q^{25} - q^{31} - q^{37} - q^{43} - q^{52} - q^{61} + q^{64} \\ & - q^{67} + 2q^{73} + 2q^{76} - q^{79} - q^{97} + q^{100} - q^{103} - q^{109} + q^{121} - q^{124} \\ & - q^{127} - q^{139} - q^{148} - q^{151} + 2q^{157} - q^{163} - q^{172} + 2q^{181} - q^{193} - q^{199} \\ & - q^{208} - q^{211} + 2q^{223} - q^{229} - q^{241} - q^{244} - 2q^{247} + q^{256} - q^{268} \\ & - q^{271} - q^{277} - q^{283} + q^{289} + O(q^{qprec}) \end{aligned}$$

We see that this conforms to what we know from question 1 and from line (1). Question 1 tells us that 19 and 73 are the primes congruent to 1 mod 3 which have 7 a cube mod p. Line (1) is confirmed by inspection, but we also make use of it (and further confirm it) down in just a bit.

Having such an f allows us to immediately know whether a rational prime p is such that 7 is a cube mod p. By number 5 we know that the conjugacy class in G of Frob_p of a prime $p \equiv 1(3)$ is either the identity or a rotation, based on whether or not $\left(\frac{7}{\pi}\right)$ is 1 or among $\{\omega$ or $\omega^2\}$, respectively. For a prime $p \equiv 2(3)$, the Frob_p is always a rotation. From 6, we know both the trace of the representation of Frob_p and that the trace is invariant per conjugacy class. Specifically, we know that

$$\mathrm{tr}(\rho(\theta)) = \begin{cases} 2, \text{ if } \theta \text{ is the identity} \\ 0, \text{ if } \theta \text{ is a reflection} \\ -1, \text{ if } \theta \text{ is a rotation} \end{cases}$$

In terms of the analysis done in problem 5 for determining the conjugacy class of Frob_p

based on p's congruence class mod 3, we have that

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = \begin{cases} 2, \text{ if } p \equiv 1(3) \text{ and } \left(\frac{7}{\pi}\right) = 1 \\ 0, \text{ if } p \equiv 2(3) \\ -1, \text{ if } p \equiv 1(3) \text{ and } \left(\frac{7}{\pi}\right) \in \{\omega, \omega^2\} \end{cases}$$

In terms of the weight one modular form of the proper level (in this case it was 1323), since the p-th coefficient a_p of q^p by the Langland conjecture introduced at the beginning of the problem is equal to $\mathrm{tr}(\rho(\mathrm{Frob}_p))$, we synthethize the previous lines to have a condition now entirely based on p(!):

$$a_p = \begin{cases} 2, \text{ if } p \equiv 1(3) \text{ and } \left(\frac{7}{\pi}\right) = 1 \\ 0, \text{ if } p \equiv 2(3) \\ -1, \text{ if } p \equiv 1(3) \text{ and } \left(\frac{7}{\pi}\right) \in \{\omega, \omega^2\} \end{cases}$$

Thus we can determine which rational primes p such that 7 is a cube mod p if $p \equiv 2(3)$ (since that is still trivial), or if $a_p = 2$. (How cool is that?!) This would mean that the other primes $p \equiv 1(3)$ for which 7 is a cube mod p up to 289 are 157, 181, 223 (but not 76 or 247 since they are not prime)!