

## Description

These problems are related to the material covered in Lectures 17-19.

**Instructions:** Pick any combination of problems to solve that sums to 100 points. Your solutions are to be written up in latex and submitted as a pdf-file via [Gradescope](#) by **midnight** on the date due.

Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on [pset partners](#), as well any references you consulted that are not posted on the course website (either in the [syllabus](#) or with the [lecture notes](#)). If there are none, write “**Sources consulted: none**” at the top of your solution. The first to spot each non-trivial typo/error in the problem sets or lecture notes will receive 1-5 points of extra credit. In cases where your solution involves code, please either include your code in your write up, or (better) the name of a notebook in your 18.783 CoCalc project containing you code (use a separate notebook for each problem).

## Problem 1. Congruence subgroups (98 points)

Let  $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$  denote the modular group and  $\mathbb{H}^* := \{\tau : \mathrm{im} \tau > 0\} \cup \mathbb{Q} \cup \{\infty\}$  the extended upper half plane. The diagram on the next page depicts a fundamental region  $\mathcal{F}$  for  $\mathbb{H}^*/\Gamma(1)$  in  $\mathbb{H}^*$ , along with nine of its translates. Each translate  $\gamma\mathcal{F}$  is labeled by  $\gamma$ , where  $\gamma$  is expressed in terms of the generators  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $T = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$  for  $\Gamma(1)$ .

The colored labels  $\rho, i, \infty$  within the region labeled by  $\gamma$  indicate the points  $\gamma\rho, \gamma i$ , and  $\gamma\infty$ , respectively (where  $\rho = e^{2\pi i/3}$ ). Note that the red, black, and blue colored  $\infty$  along the top of the diagram are all the same point, but there are three distinct translates of  $\infty$  on the real axis (at  $-1, 0, 1$ ), each of which lies in two translates of  $\mathcal{F}$  (this illustrates a key point: translates of  $\mathcal{F}$  may overlap at points whose stabilizers act non-trivially, namely, the points  $i, \rho, \infty$ ). The region  $\mathcal{F}$  includes the arc from  $i$  to  $\rho$  along the unit circle and the line from  $\rho$  to  $\infty$  along the imaginary axis, but no other points on its boundary other than  $\infty$ ; translates of these have been colored and oriented.

**Remark.** The lines/arcs connecting  $i, \rho, \infty$  in each translate of  $\mathcal{F}$  are *geodesics*, meaning they are shortest paths between two points, under the *hyperbolic metric* in which the length of a continuously differentiable path  $\gamma: [a, b] \rightarrow \mathbb{H}$  is given by  $\int_a^b \frac{|\gamma'(t)|}{\mathrm{Im}(\gamma(t))} dt$ . Such paths are necessarily either vertical lines or arcs on a semicircle that intersects the real axis in right angles. For more background on hyperbolic geometry see [2, Ch. 33].

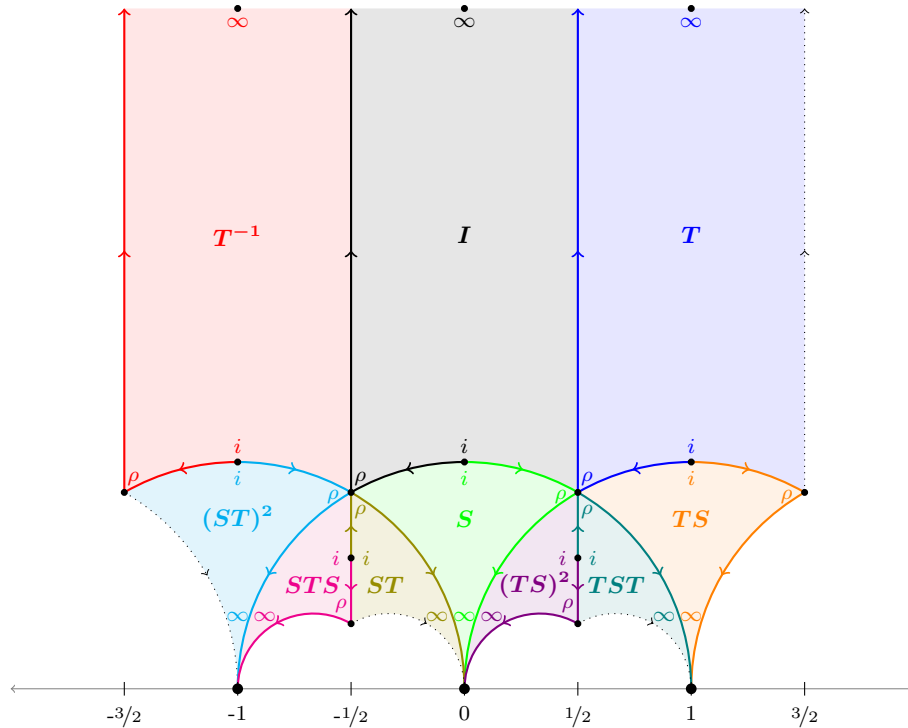
We recall the following subgroups of  $\mathrm{SL}_2(\mathbb{Z})$ , defined for each integer  $N \geq 1$ :

$$\begin{aligned}\Gamma(N) &:= \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}, \\ \Gamma_1(N) &:= \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}\}, \\ \Gamma_0(N) &:= \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}\},\end{aligned}$$

and corresponding modular curves

$$X(N) := \mathbb{H}^*/\Gamma(N), \quad X_1(N) := \mathbb{H}^*/\Gamma_1(N), \quad X_0(N) := \mathbb{H}^*/\Gamma_0(N).$$

For any congruence subgroup  $\Gamma$  we call the  $\Gamma(1)$ -translates of  $\infty$  in  $\mathbb{H}^*$  or  $\mathbb{H}^*/\Gamma$  *cusps*.



- (a) Determine the index of  $\Gamma(2)$  in  $\Gamma(1)$ , and the number of  $\Gamma(2)$  cusp orbits. Then give a connected fundamental region for  $\mathbb{H}^*/\Gamma(2)$  by listing a subset of the translates of  $\mathcal{F}$  in the diagram above and identify the cusps that lie in your region. Compute the genus of  $X$  by triangulating your fundamental region and applying Euler's formula  $V - E + F = 2 - 2g$ . Be careful to count vertices and edges correctly — initially specify vertices and edges as  $\mathbb{H}^*$ -points in the diagram (e.g.  $ST\rho$ ), then determine which vertices and edges are  $\Gamma(2)$ -equivalent (note that edges whose end points are equivalent need not be equivalent). Do the same for  $\Gamma_0(2)$  and  $X_0(2)$ .
- (b) For each of the following congruence subgroups, determine its index in  $\Gamma(1)$ , the number of cusp orbits, and a set of cusp representatives:  $\Gamma_0(3)$ ,  $\Gamma_1(3)$ ,  $\Gamma(3)$ .
- (c) Prove that for each integer  $N \geq 1$  we have an exact sequence

$$1 \longrightarrow \Gamma(N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1.$$

Show that in general one cannot replace  $\mathrm{SL}_2$  with  $\mathrm{GL}_2$  in the sequence above (so your proof for  $\mathrm{SL}_2$  needs to use more than the fact that  $\mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$  is surjective).

- (d) Derive formulas for the index  $[\Gamma(1) : \Gamma]$  for  $\Gamma = \Gamma(N)$ ,  $\Gamma_1(N)$ ,  $\Gamma_0(N)$  and any  $N \geq 1$ . Use the Euler function  $\phi(N) := \#(\mathbb{Z}/N\mathbb{Z})^\times$  where appropriate.

For any congruence subgroup  $\Gamma$ , let  $\nu_2(\Gamma)$  and  $\nu_3(\Gamma)$  count the number of  $\mathrm{SL}_2(\mathbb{Z})$  translates of  $i$  and  $\rho$ , respectively, that lie in a fundamental region of  $\mathbb{H}^*$  for  $\Gamma$  and are fixed by some  $\gamma \in \Gamma$  other than  $\pm I$ . Let  $\nu_\infty(\Gamma)$  be the number of cusp-orbits for  $\Gamma$ .

- (e) For  $\Gamma = \Gamma(p)$ ,  $\Gamma_1(p)$ ,  $\Gamma_0(p)$  derive formulas for  $\nu_2(\Gamma)$ ,  $\nu_3(\Gamma)$ ,  $\nu_\infty(\Gamma)$ , where  $p$  is a prime (hint: show that for any  $\delta \in \mathrm{SL}_2(\mathbb{Z})$ , if  $\gamma \in \mathrm{SL}_2(\mathbb{Z}) - \{\pm I\}$  stabilizes  $\delta i$  then it has trace 0, and if it stabilizes  $\delta \rho$  then it has trace  $\pm 1$ ).

Let  $\bar{\Gamma}(N), \bar{\Gamma}_1(N), \bar{\Gamma}_0(N)$  denote the images of the groups  $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$  in  $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$  respectively, and for any congruence subgroup  $\Gamma$  with image  $\bar{\Gamma}$  in  $\mathrm{PSL}_2(\mathbb{Z})$  define

$$\mu(\Gamma) := [\bar{\Gamma}(1) : \bar{\Gamma}] = \begin{cases} [\Gamma(1) : \Gamma] & \text{if } -I \in \Gamma \\ [\Gamma(1) : \Gamma]/2 & \text{if } -I \notin \Gamma \end{cases}$$

Using the Riemann-Hurwitz genus formula one can prove that for any congruence subgroup  $\Gamma$  the genus of the modular curve  $X_\Gamma := \mathbb{H}^*/\Gamma$  is given by the formula

$$g(X_\Gamma) = 1 + \frac{\mu(\Gamma)}{12} - \frac{\nu_2(\Gamma)}{4} - \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}.$$

For convenience we may write  $g(\Gamma)$  for  $g(X_\Gamma)$ .

- (f) Use your answers to (d) and (e) to give asymptotic approximations for  $g(\Gamma)$  for  $\Gamma = \Gamma(p), \Gamma_1(p), \Gamma_0(p)$  and increasing primes  $p$  that have an exact leading term (so of the form  $f(p) + O(g(p))$  for some functions  $f$  and  $g$  with  $g = o(f)$ ). Conclude that the set of primes  $p$  for which  $g(\Gamma)$  takes any fixed value is finite.

Modular curves of genus 0 and 1 are of particular interest because we can use these curves to obtain infinite families of elliptic curves over  $\mathbb{Q}$  (or a number field) that have particular properties, for example, a torsion point of order  $p$ . By Faltings' Theorem, over a number field a curve of genus  $g \geq 2$  has only a finite number of rational points.

- (g) For  $\Gamma = \Gamma(p), \Gamma_1(p), \Gamma_0(p)$  determine the primes  $p$  for which  $g(\Gamma) = 0$ , and the primes  $p$  for which  $g(\Gamma) = 1$ .

You may use Sage to check your answers (and gain intuition), but your proofs must stand on their own. To create the congruence subgroups  $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$  in Sage use `Gamma(N)`, `Gamma1(N)`, `Gamma0(N)`, respectively. The returned objects support `index()`, `nu2()`, `nu3()`, `cusps()`, and `genus()` methods that you may find useful.

## Problem 2. Non-congruence subgroups of finite index (98 points)

Recall that a *congruence subgroup* is a subgroup of  $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$  that contains  $\Gamma(N)$  for some  $N \geq 1$ . Every congruence subgroup is a finite index subgroup of  $\mathrm{SL}_2(\mathbb{Z})$ . In this problem you will prove that the converse does not hold; there exist finite index subgroups of  $\mathrm{SL}_2(\mathbb{Z})$  that are not congruence subgroups.

Let  $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ , let  $\alpha$  be the image of  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  in  $\mathrm{PSL}_2(\mathbb{Z})$ , and let  $\beta$  be the image of  $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$  in  $\mathrm{PSL}_2(\mathbb{Z})$ .

- (a) Let  $\mathbf{Z}_{2,3}$  be the finitely presented group with generators  $x, y$  satisfying the relations  $x^2 = y^3 = 1$  (and no others). Prove that the map  $\mathbf{Z}_{2,3} \rightarrow \mathrm{PSL}_2(\mathbb{Z})$  defined by  $x \mapsto \alpha$  and  $y \mapsto \beta$  is an isomorphism. You may find the diagram from Problem 1 helpful.

Part (a) implies that for any finite group  $H = \langle a, b \rangle$  with  $|a| = 2$  and  $|b| = 3$  we have a surjective group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}) \twoheadrightarrow H,$$

where the first map is quotient map  $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{PSL}_2(\mathbb{Z})$  and the second is the composition of the isomorphism  $\mathrm{PSL}_2(\mathbb{Z}) \xrightarrow{\sim} \mathbf{Z}_{2,3}$  and the surjective homomorphism  $\mathbf{Z}_{2,3} \rightarrow H$  defined by  $x \mapsto a, y \mapsto b$ . The kernel  $\Gamma_H$  of such a homomorphism is a finite index subgroup of  $\mathrm{SL}_2(\mathbb{Z})$ . Our strategy is to show that for many finite groups  $H = \langle a, b \rangle$ , this kernel cannot contain  $\Gamma(N)$  for any integer  $N$ , and is therefore not a congruence subgroup. To simplify matters, we will focus on cases where  $H$  is a *simple* group, meaning that  $H$  is a non-trivial group that contains no normal subgroups other than the trivial group and itself. Every non-trivial finite group  $G$  has a *composition series*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{k-1} \triangleleft G_k = G$$

in which each  $G_i$  is a normal subgroup of  $G_{i+1}$  and each quotient  $G_{i+1}/G_i$  is simple. The quotients  $G_{i+1}/G_i$  are called the *simple factors* of  $G$  (analogous to prime factors of an integer). This composition series is not unique, but the Jordan-Hölder theorem states that the simple factors  $G_{i+1}/G_i$  that appear in any composition series for  $G$  are unique up to isomorphism (and occur with the same multiplicity).

- (b) Prove that if a finite simple group  $S$  is a quotient of  $G$  (meaning  $S = G/K$  for some  $K \triangleleft G$ ) then  $S$  is a simple factor of  $G$  but that the converse does not hold in general.
- (c) Prove that if a finite group  $G$  is the direct product of non-trivial groups  $H_1, \dots, H_n$  then the factors of  $G$  are precisely the factors of the  $H_i$  (counted with multiplicity). Conclude that if  $S$  is a simple quotient of  $G$  then it is a quotient of one of the  $H_i$ .
- (d) Prove part (c) of Problem 1.
- (e) Let  $N = p_1^{e_1} \cdots p_r^{e_r} > 1$  by with  $p_1, \dots, p_r$  distinct primes. Prove that every simple quotient of  $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$  is a simple quotient of  $\mathrm{SL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$  for some  $i$ .
- (f) Using the fact that  $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$  is a non-abelian simple group for primes  $p \geq 5$ , show that the simple factors of  $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$  are: a cyclic group of order 2,  $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ , and  $3e - 3$  cyclic groups of order  $p$ , and that in particular,  $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$  is the unique non-abelian simple factor of  $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ , for all primes  $p \geq 5$ .
- (g) Using the fact that the alternating group  $A_n$  is a non-abelian simple group for all  $n \geq 5$ , prove that  $A_n$  is not a quotient of  $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$  for any  $N$  and any  $n > 5$ .
- (h) Using Sage, find elements  $a$  of order 2 and  $b$  of order 3 that generate  $A_9$  and list them in cycle notation. You don't need to write down a proof that they generate  $A_9$  but you should verify this in Sage. To create  $A_9$  use `A9=AlternatingGroup(9)`, and to check whether  $a$  and  $b$  generate  $A_9$  use `A9.subgroup([a,b]) == A9`.

In fact,  $A_n$  is generated by an element of order 2 and an element of order 3 for all  $n \geq 9$  (see [1]), but you are not asked to prove this. It follows from the discussion after (a) that there is a surjective homomorphism  $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow A_9$  that sends  $\pm\alpha$  to  $a$  and  $\pm\beta$  to  $b$ . The kernel  $\Gamma$  of this homomorphism is a finite index subgroup of  $\mathrm{SL}_2(\mathbb{Z})$ .

- (i) Prove that  $\Gamma$  is not a congruence subgroup.

We now want to construct a short list of generators for  $\Gamma$ . The first step is to convert the representation of  $A_9$  with generators  $a$  and  $b$  of orders 2 and 3 into a finitely presented group that is a finite quotient of  $\mathbf{Z}_{2,3}$  specified by relations. To do this use the Sage command:

```
H=A9.subgroup([a,b]).as_finitely_presented_group().simplified()
```

This may take a few seconds. The second step is to plug  $S$  and  $ST$  into all the relations in the finite presentation of  $H$  you created above. **Important:** Sage may swap the roles of  $a$  and  $b$  when it constructs the finite presentation – check the relations to see if this happened (if you see  $a^3$  and  $b^2$  in the list of relations rather than  $a^2$  and  $b^3$  then you know they were swapped). Assuming  $a^2$  and  $b^3$  are the first two relations, you can use

```
G=SL(2,Integers()); S=G([0,-1,1,0]); T=G([1,1,0,1])
for i in range(2,len(H.relations())):
    print(H.relations()[i].subs(a=S,b=S*T))
```

to get a list of matrices in  $SL_2(\mathbb{Z})$  that, together with  $S$  and  $T$  generate  $\Gamma$ . Note that the length of the list you get will depend on your choice of  $a$  and  $b$ , but shouldn't be more than 10 or 20 matrices (in fact one can do it with 4).

- (j) Record the number of matrices in your list above (not including  $S$  and  $T$ ), and a smallest and largest matrix in your list according to the  $L^\infty$ -norm (maximum of absolute values of matrix entries).

### Problem 3. Polycyclic presentations (98 points)

Let  $\vec{\alpha} = (\alpha_1, \dots, \alpha_k)$  be a sequence of generators for a finite abelian group  $G$ , and let  $G_i = \langle \alpha_1, \dots, \alpha_i \rangle$  be the subgroup generated by  $\alpha_1, \dots, \alpha_i$ . The subnormal series

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{k-1} \triangleleft G_k = G,$$

is a *polycyclic series*: each  $G_{i-1}$  is a normal subgroup of  $G_i$  and each of the quotients  $G_i/G_{i-1} = \langle \alpha_i G_{i-1} \rangle$  is a cyclic group (which we don't require to have prime order, but one can always further decompose the series so that they are). Every finite solvable group admits a polycyclic series, but we restrict ourselves here to abelian groups (written multiplicatively).

When  $G$  is the internal direct product of the cyclic groups  $\langle \alpha_i \rangle$ , we have  $G_i/G_{i-1} \cong \langle \alpha_i \rangle$  and call  $\vec{\alpha}$  a *basis* for  $G$ , but this is a special case. For abelian groups,  $G_i/G_{i-1}$  is isomorphic to a subgroup of  $\langle \alpha_i \rangle$ , but it may be a proper subgroup, even when  $G$  is cyclic.

The sequence  $r(\vec{\alpha}) = (r_1, \dots, r_k)$  of *relative orders* for  $\vec{\alpha}$  is defined by

$$r_i = |G_i : G_{i-1}|,$$

and satisfies  $r_i = \min\{r : \alpha_i^r \in G_{i-1}\}$ . We necessarily have  $r_i \leq |\alpha_i|$ , but equality typically does not hold ( $\vec{\alpha}$  is a basis precisely when  $r_i = |\alpha_i|$  for all  $i$ ). In any case, we always have  $\prod_i r_i = |G|$ , thus computing the  $r_i$  determines the order of  $G$ .

- (a) Let  $\vec{\alpha} = (\alpha_1, \dots, \alpha_k)$  be a sequence of generators for a finite abelian group  $G$ , with relative orders  $r(\vec{\alpha}) = (r_1, \dots, r_k)$ . Prove that every  $\beta \in G$  can be uniquely represented in the form

$$\beta = \vec{x} \cdot \vec{\alpha} = \alpha_1^{x_1} \cdots \alpha_k^{x_k},$$

where each  $x_i \in \mathbb{Z}$  satisfies  $0 \leq x_i < r_i$ . Show that if  $\beta = \alpha_i^{r_i}$ , then  $x_j = 0$  for  $j \geq i$ .

By analogy with the case  $r = 1$ , we call  $\vec{x}$  the *discrete logarithm* of  $\beta$  with respect to  $\vec{\alpha}$  (but note that the discrete logarithm of the identity element is now the zero vector). The vector  $\vec{x}$  can be conveniently encoded as an integer  $x$  in the interval  $[0, |G| - 1]$  via

$$x = \sum_{1 \leq i \leq k} x_i N_i, \quad N_i = \prod_{1 \leq j < i} r_j,$$

and we may simply write  $x = \log_{\vec{\alpha}} \beta$  to indicate that  $x$  is the integer encoding the vector  $\vec{x} = \log_{\vec{\alpha}} \beta$ . Note that  $x_i = \lfloor x/N_i \rfloor \bmod r_i$ , so it is easy to recover  $\vec{x}$  from its encoding  $x$ .

- (b) Design a generic group algorithm that given generators  $\vec{\alpha} = (\alpha_1, \dots, \alpha_k)$  for a finite abelian group  $G$ , constructs a table  $T$  with entries  $T[0], \dots, T[|G| - 1]$  with the property that if  $T[n] = \beta$ , then  $n = \log_{\vec{\alpha}} \beta$ . Your algorithm should also output the relative orders  $r_i$ , and the integers  $s_i$  for which  $T[s_i] = \alpha_i^{r_i}$ .

This allows us to compute a *polycyclic presentation* for  $G$ , which consists of the sequence  $\vec{\alpha}$ , the relative orders  $r(\vec{\alpha}) = (r_1, \dots, r_k)$ , and the vector of integers  $s(\vec{\alpha}) = (s_1, \dots, s_k)$ . With this presentation in hand, we can effectively simulate any computation in  $G$  without actually performing any group operations (i.e. calls to the black box). This can be very useful when the group operation is expensive.

- (c) Let  $\vec{\alpha}$ ,  $r(\vec{\alpha})$ , and  $s(\vec{\alpha})$  be a polycyclic presentation for a finite abelian group  $G$ . Given integers  $x = \log_{\vec{\alpha}} \beta$  and  $y = \log_{\vec{\alpha}} \gamma$ , explain how to compute the integer  $z = \log_{\vec{\alpha}} \beta \gamma$  using  $r(\vec{\alpha})$  and  $s(\vec{\alpha})$ , without performing any group operations. Also explain how to compute the integer  $w = \log_{\vec{\alpha}} \beta^{-1}$ .

As a side benefit, the algorithm you designed in part (b) gives a more efficient way to enumerate the class group  $\text{cl}(D)$  than we used in Problem Set 9, since the class number  $h(D)$  is asymptotically on the order of  $\sqrt{|D|}$  (this is a theorem of Siegel).

But first we need to figure out how to construct a set of generators for  $G$ . We will do this using *prime forms*. These are forms  $f = (a, b, c)$  for which  $a$  is prime and  $-a < b \leq a$  (but we do not require  $a \leq c$ , so prime forms need not be reduced). Prime forms correspond to prime ideals whose norm is prime (degree-1 primes). Recall that imaginary quadratic orders  $\mathcal{O}$  are determined by their discriminant  $D$ , which can always be written in the form  $D = u^2 D_K$ , where  $D_K$  is the discriminant of the maximal order  $\mathcal{O}_K$  and  $u = [\mathcal{O}_K : \mathcal{O}]$  is the conductor of  $\mathcal{O}$ .

- (d) Let  $a$  be a prime. Prove that if  $a$  divides the conductor then there are no prime forms of norm  $a$ , and that otherwise there are exactly  $1 + \left(\frac{D}{a}\right)$  prime forms of norm  $a$ , where  $\left(\frac{D}{a}\right)$  is the Kronecker symbol.<sup>1</sup> Write a program that, given a prime  $a$ , either outputs a prime form  $(a, b, c)$  with  $b \geq 0$  or determines that none exist.

When  $D$  is fundamental, we can generate  $\text{cl}(D)$  using prime forms of norm at most  $\sqrt{|D|/3}$ ; this follows from the bound proved in Problem Set 9 and the fact that the maximal order  $\mathcal{O}_K$  is a Dedekind domain (so ideals can be uniquely factored into prime ideals). We can still generate  $\text{cl}(D)$  with prime forms when  $D$  is non-fundamental, but bounding the primes involved is slightly more complicated, so we will restrict ourselves to fundamental discriminants for now.

<sup>1</sup>Thus  $\left(\frac{D}{2}\right)$  is 0 if  $D$  is even, 1 if  $D \equiv 1 \pmod{8}$ , and  $-1$  if  $D \equiv 5 \pmod{8}$ . Note that we refer to  $a$  as the "norm" of the form  $(a, b, c)$ , since the corresponding ideal has norm  $a$ .

- (e) Implement the algorithm you designed in part (b), using the program from part (d) to enumerate the prime forms of norm  $a \leq \sqrt{|D|/3}$  in increasing order by  $a$ . Use the prime forms as generators, but use a table lookup to discard prime forms that are already present in your table so that your  $\alpha_i$  all have relative orders  $r_i > 1$  (**warning:** prime forms need not be reduced: be sure to reduce them before making any comparisons). For the group operation, you can create binary quadratic forms in Sage using `BinaryQF([a, b, c])`, and then compose forms  $f$  and  $g$  using `h=f*g`. Use `h.reduced_form()` to get the reduced form. You will only be using this code on small examples, so don't worry about the efficiency of your implementation.
- (f) Run your algorithm on  $D = -5291$ , and then run it on the first fundamental discriminant  $D < -N$ , where  $N$  is the first five digits of your student ID. Don't list all the elements of  $\text{cl}(D)$ , just give the reduced forms for the elements of  $\vec{\alpha}$  and the integer vectors  $r(\vec{\alpha})$  and  $s(\vec{\alpha})$ . Sanity check your results by verifying that you at least get the right class number for  $D$  (you can check this in Sage using `NumberField(x**2-D, 't').class_number()`).
- (g) Recall that every finite abelian group is isomorphic to a unique product of non-trivial cyclic groups  $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$  for which  $n_1|n_2|\cdots|n_r$ . The sequence of integers  $(n_1, \dots, n_r)$  are the *invariant factors* of  $G$  and uniquely identify its isomorphism class. Design an algorithm that takes a polycyclic presentation for a finite abelian group  $G$  as input and outputs its invariant factors along with a corresponding basis  $\alpha_1, \dots, \alpha_r$  for  $G$  with  $|\alpha_i| = n_i$ .
- (h) Use your algorithm from part (g) to compute the invariant factors of the two class groups you computed in part (f), along with corresponding generators. Express each generator as a reduced form and give its discrete logarithm with respect to the generators for the polycyclic presentations you computed in part (f).

#### Problem 4. Survey (2 points)

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			

Also, please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
4/28	The modular equation				
5/3	The Hilbert class polynomial				

Please feel free to record any additional comments you have on the problem sets or lectures, in particular, ways in which they might be improved.

## References

- [1] I.M.S. Dey and J. Wiegold, *Generators for alternating and symmetric groups*, J. Australian Mathematical Society **12** (1971), 63–68.
- [2] J. Voight, *Quaternion algebras*, Springer, 2021.