Undergraduate Workshop Notre Dame 2022
Exercise sets

Andrei Jorza Evan O'Dorney Claudiu Raicu

1 Exercises for Monday

These problems are designed to give you hands-on familiarity with the material in the lectures. Some of them are easier with a computer. Don't worry if you don't have the background to solve a few of the problems; just move on.

Most of the elliptic curve problems are drawn from a handout by Bjorn Poonen at the Berkeley Math Circle.

1.1 Algebraic Curves

1. - Show that the set
   $$C = \{(t^2, t^3) : t \in \mathbf{k}\}$$
   is the same as the affine algebraic set
   $$V(y^2 - x^3).$$
   - Show then that
   $$I(C) = \langle y^2 - x^3 \rangle \subset \mathbf{k}[x, y],$$
   and conclude that C is an affine algebraic variety.
   - Show that $\dim(C) = 1$ (C is called the **cuspidal cubic curve**).
2. If X, Y are affine algebraic sets in $\mathbf{k}^n$ and I, J are ideals in A, show that
   - If $X \subseteq Y$ then $I(X) \supseteq I(Y)$.
   - If $I \subseteq J$ then $V(I) \supseteq V(J)$.
   - If we let $\sqrt{I} = \{a \in A : a^r \in I \text{ for some } r > 0\}$ denote the **radical** of the ideal I then
   $$V(I) = V(\sqrt{I}).$$
   - Using the fact that
   $$\sqrt{I} = \bigcap_{\substack{\mathfrak{P} \supseteq I \\ \mathfrak{p} \text{ prime ideal}}} \mathfrak{P}$$
   and Theorem 1.1 (see notes) show that for every ideal $I \subset A$ we have
   $$I(V(I)) = \sqrt{I}.$$

3. Show that for any two ideals $I, J \subseteq A$ we have

$$V(I \cdot J) = V(I \cap J) = V(I) \cup V(J).$$

Prove that if X is an algebraic set then we have an equivalence

$$X \text{ is irreducible } \iff I(X) \text{ is a prime ideal.}$$

4. State and prove the analogous statements in Exercises 2 and 3 for homogeneous ideals and projective algebraic sets/varieties.

5. Verify that if $X = \{[a_0 : \cdots : a_n]\}$ consists of a single point in $\mathbb{P}^n$ then the homogeneous ideal of X is

$$I(X) = \langle a_i x_j - a_j x_i : 0 \leq i < j \leq n \rangle \subset S = \mathbf{k}[x_0, \cdots, x_n],$$

and that the homogeneous coordinate ring of X is isomorphic to a polynomial ring in one variable.

By looking at specific points in $\mathbb{P}^n$, $n = 1, 2, 3, \cdots$, convince yourself that in general $I(X)$ can be generated by only n linear homogeneous polynomials (so the $\binom{n+1}{2}$ polynomials that I wrote down give in general a reduntant set of generators for $I(X)$).

6. Verify that you can decompose

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1},$$

where $\mathbb{A}^n \cong \{[1 : a_1 : \cdots : a_n]\}$ and $\mathbb{P}^{n-1} \cong \{[0 : a_1 : \cdots : a_n]\}$. We call $\mathbb{P}^{n-1}$ the **hyperplane at infinity**, parametrizing the directions of the lines through the origin in $\mathbb{A}^n$.

In fact, if we let

$$U_i = \{[a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n]\} \subset \mathbb{P}^n, \quad i = 0, \cdots, n,$$

then we can naturally identify U_i with $\mathbb{A}^n$, and its complement $H_i = \mathbb{P}^n \setminus U_i$ with $\mathbb{P}^{n-1}$.

7. Consider the subset

$$X = \{[s^3 : st^2 : t^3] : s, t \in \mathbf{k}, \text{ not both } s, t \text{ are } 0\} \subset \mathbb{P}^2 = \{[w : x : y]\}.$$

Show that

$$I(X) = \langle y^2 w - x^3 \rangle \subset \mathbf{k}[w, x, y],$$

and conclude that X is a projective variety. Using the notation in Exercise 6, show that $X \cap U_0$ is naturally identified with the cuspidal curve C in $\mathbb{A}^2 = U_0$, and that

$$X = C \cup \{[0 : 0 : 1]\},$$

where you can think of $[0 : 0 : 1]$ as the **point at infinity** on the cuspidal curve. Note also that $y^2 w - x^3$ is the **homogenization** of the equation $y^2 - x^3$ of C, with respect to the variable w.

1.2 Elliptic Curves

1. How many constants are needed in the general equation of a plane curve of degree n? (Check that your formula gives the right answer, 10, for the case $n = 3$.)

2. Let $f(x) = x^3 + Ax + B$ where A and B are real numbers. Let $\Delta = -(4A^3 + 27B^2)$. Prove that

   (a) $f(x)$ has a multiple root if and only if $\Delta = 0$.

   (b) $f(x)$ has three distinct real roots if and only if $\Delta > 0$.

   (c) $f(x)$ has one real root and two non-real roots if and only if $\Delta < 0$.

(Hint: $f(x)$ factors completely into linear factors over the complex numbers. Since there is no x^2 term in $f(x)$, the sum of the zeros of $f(x)$ is 0, and the factorization has the form

$$f(x) = (x - r)(x - s)(x + r + s)$$

for some complex numbers r and s. Calculate Δ in terms of r and s and factor it.)

The number Δ is called the *discriminant*; it plays a role analogous to that of $b^2 - 4ac$ for quadratic polynomials.

3. It turns out that the real points on the elliptic curve $y^2 = x^3 + Ax + B$ form two connected components if $\Delta > 0$ and only one connected component if $\Delta < 0$. (Loosely speaking, a connected component is a piece you can draw without lifting your pencil from the paper.) Can you explain this, using the previous problem?

4. (a) Parametrize the rational points on the hyperbola $x^2 - 2y^2 = 1$.
   (b) Find some *integer* points on this hyperbola. (In general, an equation of the form $x^2 - ky^2 = \pm 1$, where we seek integer solutions (x, y), is called a *Pell equation.*)
   (c) Prove that there are infinitely many integer points on this hyperbola. (Hint: Show that if (x_1, y_1) and (x_2, y_2) are solutions, so is $(x_1x_2 + 2y_1y_2, x_1y_2 + y_1x_2)$. Where does this formula come from?)

1.3 Modular Forms

The **Bernoulli numbers** B_n are defined by the Taylor expansion $\dfrac{x}{e^x - 1} = \sum B_n \dfrac{x^n}{n!} = 1 - \dfrac{1}{2}x + \dfrac{1}{12}x^2 - \dfrac{1}{720}x^4 + \cdots$.

1. Show that $B_n = 0$ for all **odd** $n > 1$, and that $B_n \in \mathbb{Q}$ for all n.

2. Show that

$$z \cot(z) = 1 + \sum_{n=1}^{\infty} (-4)^n B_{2n} \frac{z^{2n}}{(2n)!}$$

   [Hint: Plug in $x = 2iz$.]

3. A beautiful result from complex analysis implies that

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n \geq 1} \left(\frac{1}{z + n} + \frac{1}{z - n} \right) = \sum_{n \in \mathbb{Z}} \frac{1}{z + n}. \tag{1.1}$$

   (Same zeros and same poles!) Show that

$$z \cot(z) = 1 + 2 \sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2\pi^2}$$

   and expand into geometric series each $\dfrac{z^2}{z^2 - n^2\pi^2}$ to show that

$$\zeta(2n) = \frac{(-1)^{n+1} B_{2n} (2\pi)^{2n}}{2(2n)!}.$$

4. Let $q = e^{2\pi i z}$.

(a) Show directly from the definition of $\cot z$ that

$$\pi \cot(\pi z) = \pi i \frac{q+1}{q-1} = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n$$

(b) Differentiate equation (1.1) $k-1$ times to show that

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Undergraduate Workshop Notre Dame 2022
Exercise sets

Andrei Jorza Evan O'Dorney Claudiu Raicu

2 Exercises for Tuesday

2.1 Algebraic Curves

1. Let $S = \mathbf{k}[x_0, x_1, x_2]$ and consider irreducible homogeneous polynomials $F_1 \in S_{d_1}$, $F_2 \in S_{d_2}$, which are not scalar multiples of each other. Consider the corresponding curves $C_i = V(F_i)$, and the ideal $I = \langle F_1, F_2 \rangle$. The goal of this exercise is to compute the Hilbert function of S/I, defined by

$$HF_{S/I}(m) = \dim_{\mathbf{k}}(S/I)_m, \quad m \geq 0.$$

- Consider first the homogeneous coordinate ring $S(C_1) = S/\langle F_1 \rangle$, and verify the calculation in Example 1.3 (see notes):

$$HF_{C_1}(m) = \dim(S(C_1)_m) = \begin{cases} \binom{m+2}{2} & \text{if } m < d_1; \\ \frac{d_1 \cdot (2m+3-d_1)}{2} & \text{if } m \geq d_1. \end{cases}.$$

- Explain why multiplication by F_2 is injective on $S(C_1)$, more precisely, why it gives injective $\mathbf{k}$-linear maps

$$S(C_1)_{m-d_2} \xrightarrow{\cdot F_2} S(C_1)_m \text{ for all } m.$$

- Use the identification $S/I \cong S(C_1)/\langle F_2 \rangle$ to conclude that

$$HF_{S/I}(m) = HF_{C_1}(m) - HF_{C_1}(m - d_2) \text{ for all } m,$$

and write down an explicit formula for each m (observe the symmetry between d_1 and d_2).

- Verify that $HF_{S/I}(m) = d_1 d_2$ for $m \gg 0$, which is another formulation of Bézout's theorem.

2. (a) If X is an affine variety and $P \in X$, check that $\mathcal{O}_P \subset K^{aff}(X)$ has a unique maximal ideal, namely

$$\mathfrak{m}_P = \{f/g : f(P) = 0, g(P) \neq 0\}.$$

(b) If $X \subseteq \mathbb{P}^n$ is a projective variety, check that the set $K^{proj}(X)$ defined in Section 2 (see notes) is indeed a field. Prove that the subring $\mathcal{O}_P \subset K(X)$ has a unique maximal ideal, namely

$$\mathfrak{m}_P = \{F/G : F(P) = 0, G(P) \neq 0\}.$$

(c) Using Hilbert's Nullstellensatz, check that for both affine and projective varieties, if $P \in X$ and $\mathcal{O}_P$ is the corresponding local ring with maximal ideal $\mathfrak{m}_P$, then the natural inclusion $\mathbf{k} \subset \mathcal{O}_P$ induces an isomorphism $\mathbf{k} \simeq \mathcal{O}_P/\mathfrak{m}_P$.

(d) Prove (2.1). (See notes.)

3. Consider the projective plane curves $C_1, C_2 \subset \mathbb{P}^2$,

$$C_1 = V(X^2 + Y^2 - Z^2) \text{ and } C_2 = V(X^3 - X^2Z - XZ^2 + Z^3 - Y^2Z).$$

Determine the set $C_1 \cap C_2$ and find the intersection multiplicity at each of these points. Verify that Bézout's theorem holds in this example.

4. For a homogeneous polynomial F of degree d prove the Euler identity

$$\sum_{i=0}^{n} X_i \cdot \frac{\partial F}{\partial X_i} = d \cdot F.$$

5. Consider the cuspidal cubic $C = V(y^2 - x^3) \subset \mathbb{A}^2$.

- Show that $P = (1, 1)$ belongs to C, and that the maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_P$ is **principal**, that is, it can be generated by a single element. More precisely, show that $\mathfrak{m}_P = \langle x - 1 \rangle$ and also $\mathfrak{m}_P = \langle y - 1 \rangle$.
- By contrast, convince yourself that for $P = (0, 0)$, the ideal $\mathfrak{m}_P$ is NOT principal.

2.2 Elliptic Curves

1. Parametrize the rational points on the sphere $x^2 + y^2 + z^2 = 1$.

2. (a) Prove that the circle $x^2 + y^2 = 3$ has no rational points. (Hint: show that a rational point would give rise to a triple of integers (a, b, c) not all divisible by 3, such that $a^2 + b^2 = 3c^2$. Examine the possibilities for a, b, c modulo 3.)

   (b) Find some other integers $n > 0$ such that $x^2 + y^2 = n$ has no rational points.

3. Let X be the curve $y^2 = x^3 + x^2$.

   (a) Is X an elliptic curve?

   (b) Draw a sketch of the curve X. The point $P = (0, 0)$, where two "branches" cross, is called a *node*, which is the simplest kind of *singularity*.

   (c) Show that using lines of rational slope through the special point P yields a parametrization of the rational points on X. (You might need to exclude P and/or exclude certain slopes.)

4. Let E be the elliptic curve $y^2 = x(x + 6)(x - 6)$. Find some rational points on E, and then calculate $P + Q$ for some pairs of these to find more.

5. Let E be an elliptic curve, and let P be a point on E other than O. Show that $P + P = O$ if and only if the y-coordinate of P is zero. (This shows that in an elliptic curve, $P + P = O$ does not imply $P = O$. One cannot divide equations through by 2!)

2.3 Modular Forms

1. Show that the group $\mathrm{SL}(2, \mathbb{Z}) = \{g \in M_{2\times 2}(\mathbb{Z}) \mid \det g = 1\}$ is generated by the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. [Hint: Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Compute S^2, Sg, $T^{-q}g$ and argue by induction.]

2. For a matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$ and $z \in \mathbb{C}$ define

$$g \cdot z = \frac{az + b}{cz + d}$$

(a) Show that for any two matrices $g, h \in \mathrm{GL}(2,\mathbb{R})$, $(gh)\cdot z = g\cdot(h\cdot z)$.

(b) Show that $\mathrm{Im}(g\cdot z) = \dfrac{\det(g)\,\mathrm{Im}(z)}{|cz+d|^2}$.

(c) Deduce that $g\cdot z$ defines an action of the group $\mathrm{GL}(2,\mathbb{R})^+$ of positive determinant matrices on the upper half plane $\mathcal{H} = \{z\in\mathbb{C} \mid \mathrm{Im}\, z > 0\}$.

(d) Using calculus we may define $g\cdot\infty = \dfrac{a}{c}$. Show that the orbit of ∞ under $\mathrm{SL}(2,\mathbb{Z})$ is all of $\mathbb{Q}\cup\{\infty\} = \mathbb{P}^1\mathbb{Q}$.

3. Show that if k is odd $\mathcal{M}_k = 0$. [Hint: Write the functional equation for the matrix $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.]

4. A modular form $f\in\mathcal{M}_{2k}$ of weight[1] $2k$ with q-expansion

$$f(z) = a_0 + a_1 q + a_2 q^2 + \cdots$$

is said to be a **cusp form** if $a_0 = 0$. Denote by $\mathcal{S}_{2k}\subset\mathcal{M}_{2k}$ the sub-vector space of cusp forms. Show that

$$\mathcal{M}_{2k} = \mathbb{C}\cdot E_{2k}\oplus\mathcal{S}_{2k}.$$

This means that each modular form of weight $2k$ can be written uniquely as

$$f = \alpha E_{2k} + g$$

where $\alpha\in\mathbb{C}$ and $g\in S_{2k}$.

5. The functional equation for weight $2k$ modular forms can be rewritten as $f(g\cdot z) = (cz+d)^{2k} f(z)$ for all $g = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. If the functional equation is true for g_1 and for g_2 show that it is also true for $g_1 g_2$.

6. Check that $G_2(-\frac{1}{z}) = z^2 G_2(z) - 2\pi i z$. Taken from Serre's A Course in Arithmetic. This is quite long, your time is better spent on something else during problem-solving. Write

$$\begin{aligned}
G_2(z) &= \sum_m \left(\sum_n{}' \frac{1}{(mz+n)^2}\right)\\
\mathcal{G}_2(z) &= \sum_n \left(\sum_m{}' \frac{1}{(mz+n)^2}\right)\\
H_2(z) &= \sum_m \left(\sum_n{}' \frac{1}{(mz+n-1)(mz+n)}\right)\\
\mathcal{H}_2(z) &= \sum_n \left(\sum_m{}' \frac{1}{(mz+n-1)(mz+n)}\right)
\end{aligned}$$

where $\sum'$ means over all indices where the terms in the sum don't have a 0 in the denominator.

(a) Show that $H_2(z) = 2$ and $\mathcal{H}_2(z) = 2 - \frac{2\pi i}{z}$.

(b) Show that $G_2 - H_2$ and $\mathcal{G}_2 - \mathcal{H}_2$ converge absolutely, and therefore they must equal each other.

(c) Conclude that $G_2(-\frac{1}{z}) = z^2 G_2(z) - 2\pi i z$.

[1] The previous exercise shows that there are no odd weight modular forms

Undergraduate Workshop Notre Dame 2022
Exercise sets

Andrei Jorza Evan O'Dorney Claudiu Raicu

3 Exercises for Wednesday

3.1 Elliptic Curves

1. Find an elliptic curve with a rational point $P \neq O$ satisfying $P+P+P=O$. Hint: if a line L intersects E only at a single point P, and in particular does not pass through O (i.e., it is not vertical and is not the line at infinity), then by Bezout's Theorem, $L \cap E$ must be P with multiplicity 3, so $P+P+P=0$.
2. Let C be the curve $y^2+y=x^3-x^2$.
   (a) Is C an elliptic curve? (Hint: Try to change coordinates so that the y term disappears.)
   (b) Find some integral points P on C.
   (c) Prove that the points you found are *torsion points,* that is, there is an integer n such that $nP=0$.
3. Let $p \neq 2$ be a prime number. Consider the problem of finding the number of solutions to the quadratic congruence $x^2-y^2 \equiv 1 \mod p$, for integers x, y modulo p.
   (a) Compute some examples and conjecture the answer.
   (b) How does a rational parametrization for the curve $C: x^2-y^2=1$ help?
   (c) If you are familiar with algebra in the *finite field* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, prove your conjecture.
4. Compute the points on the curve $y^2 \equiv x(x+5)(x-5) \mod p$, for a prime p of your choosing ($p \neq 2, 5$), and write the group structure on them in the form $\mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_r\mathbb{Z}$.

Undergraduate Workshop Notre Dame 2022
Exercise sets

Andrei Jorza Evan O'Dorney Claudiu Raicu

4 Exercises for Thursday

4.1 Algebraic Curves

1. Let $C = \mathbb{P}^1$ with projective coordinates $[X : Y]$, and consider the rational function

$$t = Y/X \in K(\mathbb{P}^1).$$

(a) Show that $K(\mathbb{P}^1) = \mathbf{k}(t)$, and compute the principal divisor $\mathrm{Div}(t)$.

(b) Show that if $E = \sum_P a_P \cdot P$ is an effective divisor on $\mathbb{P}^1$ of degree d, then there exists a homogeneous polynomial F of degree d with $\mathrm{Div}(F) = E$.

(c) Explain how to compute the divisor of an arbitrary rational function on $\mathbb{P}^1$.

(d) Show that $\mathrm{Cl}(\mathbb{P}^1) = \mathbb{Z}$ and $\mathrm{Cl}^0(\mathbb{P}^1) = 0$.

(e) For the rational function $t = Y/X$, determine $l(r \cdot \mathrm{Div}_0(t))$ for all $r \geq 0$.

(f) Verify that Proposition 1.6 holds for $C = \mathbb{P}^1$.

2. Fix a constant $\lambda \in \mathbf{k}$ with $\lambda \neq 0, 1$ and consider the cubic $E \subset \mathbb{P}^2$ defined by the equation

$$Y^2Z = X \cdot (X - Z) \cdot (X - \lambda Z).$$

Consider the rational functions $x = X/Z$ and $y = Y/Z$.

(a) Show that $K(C) = \mathbf{k}(x, y)$ (where x, y satisfy the relation $y^2 = x(x-1)(x-\lambda)$).

(b) Determine $\mathrm{Div}(x)$ and $\mathrm{Div}(y)$.

(c) Show that if you let $z = x^{-1}$ then $L(\mathrm{Div}_0(z)) \subset \mathbf{k}[x, y]$ and prove that

$$l(r \cdot \mathrm{Div}_0(z)) = 2r \text{ for all } r > 0.$$

3. We say (see the notes) that D and D' are **linearly equivalent** if $D' - D = \mathrm{Div}(h)$ is a principal divisor, and write $D \equiv D'$. Show the following:

- $l(D) > 0 \iff D$ is linearly equivalent to an effective divisor.
- $\deg(D) = 0$ and $l(D) > 0 \iff D \equiv 0 \iff D$ is a principal divisor.

4. In this exercise you will prove (you can also look at the notes to see the details) that if $D \leq D'$ are divisors on a curve C then

$$l(D') \leq l(D) + \deg(D' - D).$$

- Explain why you can reduce to the case when $D' - D = P$ consists of a single point.
- Let a be the coefficient of P in D (so that $(a+1)$ is the coefficient of P in D'), and let π denote the uniformizer at P (so that $\mathfrak{m}_P = \langle \pi \rangle$). Explain why the map

$$\phi : L(D') \longrightarrow \mathbf{k}, \quad \phi(f) = (f \cdot \pi^{a+1})(P),$$

  defined by multiplication by π^{a+1} followed by evaluation at P, is $\mathbf{k}$-linear and is well-defined.
- Show that $L(D)$ is contained in $\ker(\phi)$ and deduce that $l(D') \leq l(D) + 1$.

5. (**Prime avoidance**) Suppose that $J, Q_0, Q_1, \cdots, Q_r$ are ideals in a ring R, and assume further that $Q_1, \cdots, Q_r$ are prime ideals (Q_0 may not be prime). Show that if we have

$$J \subseteq Q_0 \cup Q_1 \cup \cdots \cup Q_r$$

then $J \subseteq Q_i$ for some i. You can follow the strategy below:

(a) Verify the assertion in the case $r = 0, 1$.

(b) Do induction on r. If $J \subset \bigcup_{j \neq i} Q_j$ then conclude by induction that $J \subset Q_j$ for some j. Otherwise, for each $i = 0, \cdots, n$ choose an element $z_i \in J \setminus \bigcup_{j \neq i} Q_j$. Show that the element $z = z_0 z_1 \cdots z_{r-1} + z_r$ belongs to J but not to any of Q_i.

6. Prove Lemma 1.5 using Proposition 1.4.

4.2 Modular Forms

1. Show that if $f \in M_{2k}$ and $g \in M_{2\ell}$ are modular forms then $fg \in M_{2k+2\ell}$ is also a modular form. (Pay attention to the weights.)

2. Show that $\Delta, E_{12}, E_4^3, E_6^2 \in M_{12}$. We showed that M_{12} has dimension at most 2.

   (a) From lectures, and some computations, we know that

$$\begin{aligned} 19200 E_4^3 &= \frac{1}{720} + q + 249q^2 + \cdots \\ 252 E_6^2 &= \frac{1}{1008} - q + 219q^2 + \cdots \\ \Delta &= q - 24q^2 + \cdots \\ E_{12} &= \frac{691}{65520} + q + 2049q^2 + \cdots \end{aligned}$$

   Show that E_4^3 and E_6^2 are linearly independent, and therefore form a basis of M_{12}.

   (b) Find two constants $a, b \in \mathbb{C}$ (you can do this by hand) such that

$$\Delta - E_{12} = 19200 E_4^3 \cdot a + 252 E_6^2 \cdot b.$$

   (c) Conclude the beautiful relation, from lecture, that

$$\Delta = E_{12} - \frac{691}{13}(1600 E_4^3 + 21 E_6^2),$$

   which led us to a proof of Ramanujan's congruence mod 691.

3. Consider the modular form $\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$ of weight 12.

(a) Show that Δ has no zeros in $\mathcal{H}$. [Hint: Recall that $\frac{d \log \Delta(z)}{dz} = \frac{6i}{\pi} G_2(z)$. Any root of $\Delta(z)$ would have to be a pole of this log derivative. Does $G_2(z)$ ever not converge in $\mathcal{H}$?]

(b) Suppose $f \in S_{2k}$ is a modular form with constant term 0 (a cusp form, as in the previous set). Show that $\dfrac{f}{\Delta}$ is analytic in $\mathcal{H}$ and at ∞.

(c) Deduce that $\mathcal{M}_k \xrightarrow{\cdot\Delta} \mathcal{S}_{k+12}$ is a bijection.

(d) Conclude that

$$\dim \mathcal{M}_{2k} = \begin{cases} \lfloor 2k/12 \rfloor + 1 & 2k \not\equiv 2 \pmod{12} \\ \lfloor 2k/12 \rfloor & 2k \equiv 2 \pmod{12} \end{cases}.$$

Undergraduate Workshop Notre Dame 2022
Exercise sets

Andrei Jorza Evan O'Dorney Claudiu Raicu

5 Exercises for Friday

5.1 Algebraic Curves

1. Let $C = \mathbb{P}^1$ (genus $g = 0$). Explain why you can take the canonical divisor W to be any divisor of degree -2 in the Riemann–Roch theorem.

2. (a) Show that in the Riemann–Roch theorem, you can replace W with any linearly equivalent divisor $W' \equiv W$.

   (b) Suppose that E is an elliptic curve (genus $g = 1$). Use the fact that $l(W) = g$ to show that W is linearly equivalent to an effective divisor, and determine this divisor using $\deg(W) = 2g - 2$.

   (c) Conclude that for an elliptic curve, you can take $W = 0$ in the Riemann–Roch theorem.

3. Let E be an elliptic curve, and fix $O \in E$. The goal of this exercise is to show (see also the notes) that we have a bijection
$$\phi : E \longrightarrow \mathrm{Cl}^0(E), \quad \phi(P) = P - O.$$
   - Surjectivity: every element of $\mathrm{Cl}^0(E)$ is the equivalence class of a divisor D with $\deg(D) = 0$. Use Riemann–Roch to conclude that $l(D + O) = 1$, and conclude that $D + O$ is equivalent to an effective divisor of degree 1 (what does such a divisor look like?).
   - Injectivity: show that if $P - O \equiv Q - O$, $P \neq Q$, then $L(P - Q)$ contains a non-constant rational function f. Explain why this implies $1, f \in L(P)$, and $l(P) \geq 2$. Show that this contradicts Riemann–Roch, so ϕ is in fact injective.

4. Let C be a curve of genus g and let $P \in C$. Show that for every $a \geq 2g$ there exists a rational function $f \in K(C)$ with
$$\mathrm{Div}_\infty(f) = a \cdot P.$$
   Prove that the above conclusion fails when a is small (for instance when $a = 1$ and C is any curve of genus $g \geq 1$).

5. Let C be a curve of genus g, let $P \in C$, and define
$$N_r = l(rP) \text{ for } r \geq 0.$$
   (a) Show that $1 = N_0 \leq N_1 \leq \cdots \leq N_{2g-1} = g$ and conclude that there are precisely g numbers
$$0 < a_1 < a_2 < \cdots < a_g < 2g$$
   with the property that there is no rational function $f \in K(C)$ with $\mathrm{Div}_\infty(f) = a_i \cdot P$.

The numbers $a_1, \cdots, a_g$ are called **Weierstrass gaps**, and $(a_1, \cdots, a_g)$ is the **gap sequence at** P. We say that P is a **Weierstrass point** if the gap sequence is different from $(1, 2, \cdots, g)$.

(b) Show that the following are equivalent

- P is a Weierstrass point.
- $l(gP) > 1$.
- $l(W - gP) > 0$.

(c) Show that if a and b are not gaps then $a + b$ is not a gap. Conclude that if 2 is not a gap then the gap sequence is necessarily $(1, 3, \cdots, 2g - 1)$. The curve C is called **hyperelliptic** in this case.

5.2 Modular Forms

1. A little more computation, you can skip this if you are tired of computations, but the whole reason for this exercise is to apply the result to the next one, which is a really wonderful arithmetic identity. Recall that $\sigma_k(n) = \sum_{d|n} d^k$.

$$\begin{aligned}
240E_4 &= 1 + 240(q + 9q^2 + \cdots) = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n \\
(240E_4)^2 &= 1 + 480q + 61920q^2 + \cdots \\
(240E_4)^3 &= 1 + 720q + 179280q^2 + \cdots \\
-504E_6 &= 1 - 504(q + 33q^2 + \cdots) = 1 - 504\sum_{n=1}^{\infty} \sigma_5(n)q^n \\
(-504E_6)^2 &= 1 - 1008q + 220752q^2 + \cdots \\
480E_8 &= 1 + 480(q + 129q^2 + \cdots) = 1 + 480\sum_{n=1}^{\infty} \sigma_7(n)q^n \\
-264E_{10} &= 1 - 264(q + 513q^2 + \cdots) = 1 - 264\sum_{n=1}^{\infty} \sigma_9(n)q^n
\end{aligned}$$

   Show that

$$\begin{aligned}
480E_8 &= (240E_4)^2 \\
-264E_{10} &= (240E_4) \cdot (-504E_6)
\end{aligned}$$

2. Use the previous exercise to show that

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040\sum_{k=1}^{n-1} \sigma_3(k)\sigma_5(n-k)$$

   (Think about how surprising this is: $\sigma_7(2) = 1 + 2^7$, $\sigma_3(2) = 1 + 2^3$ so we are saying that $1 + 2^7 = 1 + 2^3 + 120 \cdot 1$.)

3. Show that every modular form (of weight ≥ 4 and level 1) can be written as a polynomial in E_4 and E_6. [Hint: Remember that cusp forms are multiples of Δ so you can argue by induction.]

4. Suppose $f(z) \in M_{2k}(N)$. If M is a positive integer, show that $g(z) = f(Mz) \in M_{2k}(MN)$.