KIDDIE TALK: THE FIVE ELEMENTARY OPERATIONS ACCORDING TO EICHLER

EVAN WARNER

According to a quote attributed to Eichler, the five elementary mathematical operations are addition, subtraction, multiplication, division, and modular forms. Assuming people are familiar with the first four, I will discuss a few applications of modular forms.

1. Basic concepts

Modular forms are functions, so they are defined on some space. In this case, the space is the upper complex half plane

$$\mathcal{H} = \{x + iy \in \mathbb{C} : y > 0\}.$$

This space is nice in a surprising number of ways. It has a nice hyperbolic metric on it (the Poincaré metric), for instance. For our purposes, the most important property is that it admits a nice action of the group $G = \mathrm{SL}_2(\mathbb{R})$, defined by Möbius transformations as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

We can see easily that G (as a Lie group) acts continuously and transitively on $\mathcal{H}$; in other words, $\mathcal{H}$ is a homogeneous space for G. We make the following notational definition: for a positive integer N, let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod N \right\}.$$

Then $\Gamma_0(N)$ is a discrete subgroup of G. Note that $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

Now we make three choices that determine our space of modular forms.[1] We pick an integer k, called the *weight*, a positive integer N, called the *level*, and a Dirichlet character $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, called the *nebentypus*. If you've never seen modular forms before, you should immediately specialize to the easiest case $N = 1$, in which case χ is also necessarily trivial.

Given these three choices, a *modular form* $f : \mathcal{H} \to \mathbb{C}$ is a function satisfying the following three criteria:

- The function f is holomorphic on $\mathcal{H}$,
- The function f is holomorphic "at the cusps" (to be explained below), and
- The function f transforms nicely in the following way: for every

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

[1] These choices can be generalized considerably by replacing $\Gamma_0(N)$ with other discrete subgroups of G, but we won't need to for this talk.

and for any $z \in \mathcal{H}$, we have

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z). \tag{1}$$

Let $M_k(N,\chi)$ denote the set of modular forms of weight k, level N, and nebentypus χ. Clearly, $M_k(N,\chi)$ is a $\mathbb{C}$-vector space. Another way of describing (1) is the following: we can define an action of $\Gamma_0(N)$ on the set $\mathcal{O}(\mathcal{H})$ of holomorphic functions f on $\mathcal{H}$ by

$$(f|_{k,\chi}\gamma)(z) = \chi(d)^{-1}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

for $\gamma \in \Gamma_0(N)$. Therefore we have a representation of $\Gamma_0(N)$ on $\mathcal{O}(\mathcal{H})$, and $M_k(N,\chi)$ is precisely the set of $\Gamma_0(N)$-invariant functions.

Let's look more closely at the case $N = 1$. It is not difficult to see that a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ is given by

$$\mathcal{F} = \left\{ z \in \mathcal{H} : |z| > 1, |\mathrm{re}(z)| < \frac{1}{2} \right\}$$

(by this, we mean that at least one representative of $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$ lies in $\overline{\mathcal{F}}$, and at most one representative of $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$ lies in $\mathcal{F}^\circ$). The closure of this domain is not compact: it goes off to ∞. We say that ∞ is a *cusp* of $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$.

We can check that f is holomorphic at the cusp in one of two ways: first, we could compactify $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$ by adding a point at infinity, which somewhat miraculously allows us to put a complex structure on the set (so we end up with a compact Riemann surface); holomorphicity at the cusp then just means that f has a removable singularity there. Alternatively, because this is a somewhat annoying procedure, we note that by taking the matrix

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

and plugging it into (1), we get

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

Thus f is periodic, and (since it's certainly smooth enough!) has a Fourier expansion

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n z}.$$

The condition that f is holomorphic at ∞ is exactly the condition that $a_n = 0$ if $n < 0$; that is, $f(z)$ can be expressed as a power series in $q = e^{2\pi i z}$. In more general cases (i.e., $N \neq 1$), we have to conjugate a cusp to ∞ first so we can take its Fourier expansion, but otherwise the picture is identical.

One additional note for the $N = 1$ case (though it can be immediately generalized): if $k = 0$, then we're asking for a function f that is *invariant* under $\mathrm{SL}_2(\mathbb{Z})$ and holomorphic everywhere (including at any cusps). A holomorphic function on a compact Riemann surface is constant (Liouville's theorem). Therefore $M_0(1) = \mathbb{C}$, the constant functions. An argument with basic complex analysis shows that $M_k(1) = \emptyset$ if $k < 0$. Therefore if we want interesting modular forms, we'd better use a positive weight.

In all cases, a simple argument that counts zeroes using Cauchy's theorem shows that the space $M_k(N,\chi)$ is finite-dimensional: using a contour approximately traversing a fundamental domain, we find that the total order of vanishing of a modular form is bounded, which quickly implies finite-dimensionality. This is of fundamental importance in the sequel.

2. Basic strategy for applications of modular forms

Okay, here's the basic strategy. We have a sequence of numbers we don't know much about. Somehow, we figure out that they form Fourier coefficients of a modular form in $M_k(N, \chi)$. By finite-dimensionality, we can figure out exactly which modular form we've got algorithmically (in terms of a sum of simpler modular forms, as will be described below in certain cases). Then we potentially know much more about our sequence of numbers.

3. Eisenstein series and sum-of-divisors relations

Here is the simplest possible application of the basic strategy. We don't know any nontrivial modular forms yet, so part of this application will be to show that we can, in fact, actually write some down.

If we have a representation $\rho : G \to \mathrm{End}(V)$ of a group G on a vector space V, a good way of forming invariant vectors is to start with an arbitrary vector $v_0 \in V$ and form the sum

$$v = \sum_{g \in G} \rho(g) \cdot v_0.$$

If v_0 is already invariant under a subgroup G_0, then we can instead simply sum over the cosets $G_0 \setminus G$:

$$v = \sum_{g \in G_0 \setminus G} \rho(g) \cdot v_0.$$

Let's apply this in our simple case, where $G = \mathrm{SL}_2(\mathbb{Z})$ and $V = \mathcal{O}(\mathcal{H})$. Note that if v is 1-periodic, hence invariant under T, we can take G_0 to be $\langle T \rangle$. The resulting function, if the sum converges, is known as a Poincaré series. Let's specify now to $N = 1$ and $v = 1$ (the constant function). It is an easy exercise that our Poincaré series in this case becomes

$$E_k(z) = \sum_{\gamma \in \langle T \rangle \setminus G} 1|_k\gamma = \frac{1}{2} \sum_{\substack{c,d \in \mathbb{Z} \\ (c,d)=1}} \frac{1}{(cz+d)^k}$$

This is called the *Eisenstein series of weight k.* It converges to a nonzero value whenever k is even and ≥ 4.

Here are the two main theorems about Eisenstein series. Neither is difficult to prove, but neither are particularly interesting either.

Theorem 3.1. *The Fourier expansion of E_k is given by*

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2\pi i n z},$$

where B_k is the kth Bernoulli number and $\sigma_{k-1}(n)$ denotes the sum of the $(k-1)$st powers of the positive divisors of n.

Proof sketch. The standard proof of this expansion starts with the partial fraction decomposition of the cotangent function

$$\pi \cot(\pi z) = \sum_{n \in \mathbb{Z}} \frac{1}{z+n}$$

and repeatedly differentiates. Simple algebra suffices from here, plus Euler's evaluation of positive even integer values of the zeta function in terms of Bernoulli numbers. □

For the next result, note that if $f \in M_k(1)$ and $g \in M_\ell(1)$, then $f \cdot g \in M_{k+\ell}(1)$. Therefore the set of all modular forms $M_*(1)$ for $\mathrm{SL}_2(\mathbb{Z})$ forms a graded ring, with the grading given by the weight.

Theorem 3.2. *As graded rings, $M_*(1) = \mathbb{C}[E_4, E_6]$, where E_4 has degree 4 and E_6 has degree 6.*

Proof sketch. One proves that E_4 and E_6 are algebraically independent and uses explicit dimension bounds (given using Cauchy's formula as described above) to show that they generate all modular forms. □

In particular, there are no modular forms for $\mathrm{SL}_2(\mathbb{Z})$ of weight < 4 or of odd weight.

These two theorems together imply that there exist some interesting relations between the functions $\sigma_k(n)$. For example, consider E_4^2 and E_8, which are both modular forms of weight 8. According to Theorem 3.2, $M_8(1)$ is one-dimensional, so the two series must be proportional. But they both have constant term one, so in fact we have

$$E_4^2 = E_8.$$

This is an example of our basic strategy: to verify any relation between modular forms, we only have to check a finite amount of information (here, just the constant terms of the Fourier expansions). Now look back at the full Fourier series for both sides of this equation, and note that $B_4 = B_8 = -\frac{1}{30}$. The Fourier expansion of E_4^2 is

$$\left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) e^{2\pi i n z}\right)^2 = 1 + \sum_{n=1}^{\infty} \left(240^2 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m) + 480\sigma_3(n)\right) e^{2\pi i n z},$$

so by comparison to the Fourier expansion of E_8 we conclude that

$$240^2 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m) + 480 \cdot \sigma_3(n) = 480 \cdot \sigma_7(n),$$

or, simplifying,

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

To demonstrate the purely algorithmic nature of these computations, I wrote a computer program to derive Eisenstein series relations and the corresponding sum-of-divisor relations. All that is necessary is some linear algebra (and the ability to compute Bernoulli numbers). For example, my program informs me that

$$E_{28} = \frac{489693897}{3392780147} E_4^7 + \frac{2507636250}{3392780147} E_4^4 E_6^2 + \frac{395450000}{3392780147} E_4 E_6^4.$$

If we define

$$\sigma_{k-1}(0) = -\frac{B_k}{2k}$$

(a convention due to Ramanujan), write $*$ to denote discrete convolution of functions, and adopt the convention that all powers are repeated convolution (not pointwise exponentiation), then the program finds the corresponding sum-of-divisors identity

$$\sigma_{27}(n) = \frac{935819610457373472000000}{29}\sigma_3^7(n) + \frac{8805607783096320000000}{29}(\sigma_3^4 * \sigma_5^2)(n) + \frac{25516066518835200000}{29}(\sigma_3 * \sigma_5^4)(n).$$

While results like these can be derived purely combinatorially, the proofs are very much more complicated.

We can find more relations between sum-of-divisors functions by finding other relations between Eisenstein series; one fruitful method is by considering various differential operators on $M_k(1)$. We will not pursue this line of thought here.

4. Sums of squares

Let $r_m(n)$ denote the number of solutions in integers to the equation

$$\sum_{i=1}^{m} x_i^2 = n.$$

That is, $r_m(n)$ is defined to be the number of representations of an integer n as a sum of m squares. The study of $r_m(n)$ is a classical one, going back to Fermat and Euler ($m = 2$), Lagrange ($m = 4$), and Jacobi ($m = 6, 8$). We will consider the case of m even, because it is much easier and much more amenable to our methods.

One tried and true method of analyzing sequences of numbers is to consider their generating functions; i.e., the power series that has our sequence as its coefficients. Let

$$\theta(z) = \sum_{j\in\mathbb{Z}} q^{j^2} = 1 + 2q + 2q^4 + 2q^9 + \ldots;$$

this is the simplest Jacobi theta function and we clearly have

$$\theta(z) = \sum_{n\geq 0} r_1(n) q^n.$$

That is, $\theta(z)$ is the generating function for $r_1(n)$. Obviously, $\theta(z + 1) = \theta(z)$. Perhaps less obviously, we have the transformation formula

$$\theta\left(-\frac{1}{4z}\right) = \sqrt{\frac{2z}{i}}\theta(z). \tag{2}$$

This can be proven by applying the Poisson summation formula to the Gaussian function $f(x) = e^{-\pi t x^2}$, which yields

$$\sum_{j\in\mathbb{Z}} e^{-\pi j^2 t} = \frac{1}{\sqrt{t}} \sum_{j\in\mathbb{Z}} e^{-\pi j^2/t}.$$

This immediately gives (2) for the positive imaginary axis, and the result follows by analytic continuation.

At this point we make two important observations: first, we note that by expanding, $\theta(z)^m$ is the generating function for $r_m(n)$. And second, the transformation rules for $\theta(z)$ imply that $\theta(z)^2$ is a modular form of weight 1, level 4, and nebentypus $\chi = \chi_{-4}$, where χ_{-4} is the Dirichlet character modulo 4 given by

$$\chi_{-4}(n) = \begin{cases} 1 & \text{if } n \equiv 1 \mod 4, \\ -1 & \text{if } n \equiv 3 \mod 4, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore $\theta(z)^{2k} \in M_k(4, \chi^k)$.

To carry out the same procedure as before and determine what $r_m(n)$ is more exactly, we want analogues of the Eisenstein series for $M_k(4, \chi^k)$. In this case we don't have a theorem like Theorem 3.2, but we can still try to express $\theta(z)^{2k}$ as a linear combination of Eisenstein series. Here there are two relevant Eisenstein series of each level instead of just one, given by

$$E'_{k,\chi_{-4}} = 1 + \frac{2}{L(1-k,\chi)} \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi(d) d^{k-1} \right) e^{2\pi i n z}$$

and

$$E''_{k,\chi_{-4}} = 1 + \frac{2}{L(1-k,\chi)} \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi\left(\frac{n}{d}\right) d^{k-1} \right) e^{2\pi i n z}.$$

Here the Fourier coefficients are suitably twisted analogues of $\sigma_d(n)$ and the L-function special values $L(1-k,\chi)$ can be calculated in much the same way as zeta function special values (for example, $L(0,\chi) = \frac{1}{4}$).

The big fact (proven merely by counting dimensions, which can be done most naturally with the Riemann-Roch theorem) is that for k less than or equal to 4, $S_k(4, \chi^k) = \emptyset$. Therefore we can express any element of these spaces as a linear combination of Eisenstein series. Finitely much simple arithmetic therefore yields the following:

$$\begin{aligned} r_2(n) &= 4 \sum_{d|n} \chi(n), \\ r_4(n) &= 8(2 + (-1)^n) \sum_{d|n, 2\nmid d} d, \\ r_6(n) &= 16 \sum_{d|n} \chi\left(\frac{n}{d}\right) d^2 - 4 \sum_{d|n} \chi(d) d^2, \\ r_8(n) &= 16 \sum_{d|n} (-1)^{n-d} d^3. \end{aligned}$$

Unfortunately, for $k > 4$ we also have to consider cusp forms, and it is much more difficult to write down explicit examples of these (hence, it is more difficult to write down explicit formulae for r_{2k} in that instance). However all is not lost: as it turns out, the Fourier coefficients of cusp forms increase considerably more slowly than the Fourier coefficients of Eisenstein series, so by finding the part of $\theta(z)^{2k}$ which is spanned by Eisenstein series goes a long way towards finding good asymptotics for $r_{2k}(n)$ or representation numbers for arbitrary positive definite quadratic forms.

5. Milnor's example

To any positive definite quadratic form, we can associate a generating function, which will turn out to be a modular form (though of a slightly more general type than we have been considering, because we will have to include modular forms of half-integer weights). There are some special quadratic forms that are modular forms for the full modular group $\mathrm{SL}_2(\mathbb{Z})$, and a couple of these have an unexpected application to the old question: "Can you hear the shape of a drum?"

Let

$$Q(x) = \frac{1}{2} x^t A x$$

be a very special positive definite quadratic form in m variables, where both A and A^{-1} are symmetric matrices with integer elements and even integer elements on the diagonal. Such quadratic forms are called *even unimodular*, and they necessarily satisfy $m \equiv 0 \mod 8$. Each is associated in the usual way to a lattice. The general theorem on modularity of theta series then gives

Theorem 5.1. *If $Q(x)$ is an even unimodular positive definite quadratic form in m variables, then the associated theta series*

$$\theta_Q(z) = \sum_{j \in \mathbb{Z}^m} q^{Q(j)}$$

is an element of $M_{m/2}(1)$; that is, a modular form for the full modular group of weight $m/2$.

Although it is by no means obvious that such lattices always exist, it can be shown (using the Siegel mass formula, whose proof involves modular forms!) that if m is large, there are very many such indeed. In fact, for $m = 32$ it is known that more than 80 million isomorphism classes of even unimodular lattices exist.

For this example, we take it as a given that there are two distinct even unimodular lattices of rank $m = 16$; they are usually called $\Lambda_8 \oplus \Lambda_8$ and Λ_{16}. By Theorem 5.1, their corresponding theta series lie in $M_8(1)$. But they both have leading coefficient one (because zero has only one representation by a positive definite quadratic form) and $\dim M_8(1) = 1$, so in fact

$$\theta_{\Lambda_8 \oplus \Lambda_8}(z) = \theta_{\Lambda_{16}}(z).$$

That is, the two nonismorphic lattices have equal representation numbers.

This is just a nice curiosity until one notices the following: since the two lattices are not isomorphic, the corresponding tori

$$M_1 = \mathbb{R}^{16}/(\Lambda_8 \oplus \Lambda_8)$$

and

$$M_2 = \mathbb{R}^{16}/\Lambda_{16}$$

are not isometric as Riemannian manifolds. But the spectrum of the Laplace operator on any torus $\mathbb{R}^n/\Lambda$ is just the set of norms of elements of the lattice, counted with multiplicities. So the fact that the representation numbers coincide implies that these two non-isometric manifolds M_1 and M_2 have the same spectrum. In other words, we cannot discern the shape of these sixteen-dimensional drums merely by looking at their spectra. This was the first example found of this phenomenon, and as far as I am aware by far the simplest.

6. How to generalize your modular forms

Here's a few ways that these ideas generalize. We started with the upper half plane $\mathcal{H}$, but we really should have started with the group $G = \mathrm{SL}_2(\mathbb{R})$, because given G we could have recovered $\mathcal{H}$ as follows. Take a maximal compact subgroup K of G (all of which are conjugate to $K = \mathrm{SO}_2(\mathbb{R})$, so we might as well take that), and take the natural action of G on G/K. Amazingly, we recover exactly the action of G on $\mathcal{H}$ that we had earlier! So we needn't have thought of modular forms as certain functions on $\mathcal{H}$ at all, convenient though that undoubtedly was: we could have thought of them as certain functions on G itself that are invariant under $\mathrm{SO}_2(\mathbb{R})$.

This paves the way for doing the same procedure for arbitrary Lie groups G: we take a maximal compact K, form the symmetric space G/K, take a discrete subgroup thereof, and go to town as analogously as we can. There is a slight subtlety here: G/K may not have a canonical complex structure on it.[2] So this broadening of perspective also requires that we abandon our requirement of holomorphicity. In its place, we generally require that our functions be eigenfunctions of some appropriate analogue of the Laplace operator, which is more general.[3]

Finally, we wrap everything up in adelic language, which allows us to easily generalize to other number fields (the above being the $F = \mathbb{Q}$ case, more or less). And all of a sudden, you're studying modern automorphic forms.

7. References

Bruinier, van der Geer, Harder, Zagier, *The 1-2-3 of Modular Forms*, Springer, 2008.

Iwaniec, *Topics in Classical Automorphic Forms*, American Mathematical Society, Graduate Studies in Mathematics vol. 17, 1997.

[2] In fancy language, the symmetric space G/K may not be a Hermitian symmetric space.

[3] The appropriate analogue turns out to be various Casimir operators on G.