

Introduction to Modular Forms

Samuele ANNI

Aix-Marseille Université
France

16–21 July 2025

Arithmetic in Action: Number Theory
and its Applications to Cryptography and Coding Theory
Universitas Gadjah Mada

Outline

- 1 Eisenstein Series of Weight 2
- 2 Counting Representations
- 3 The Serre Derivative
- 4 Congruences
- 5 Modular Forms of Higher Level
- 6 Hecke Operators

Eisenstein Series of Weight 2

In the definition of $G_k(z)$, we required $k > 2$ to ensure absolute convergence of the series.

However, the q -series

$$G_k(z) = \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

also makes sense for $k = 2$ and defines a holomorphic function on the upper half plane H . We define the Eisenstein series of weight 2 by:

$$G_2(z) := \zeta(2) + (2\pi i)^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n$$

This function is holomorphic on H , but it is **not** a modular form.

Nonetheless, G_2 plays a crucial role in the theory of modular forms and quasi-modular forms.

Failure of Modularity of G_2

We have the following transformation property:

Proposition 1 (Modular transformation of G_2)

For all $z \in H$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have:

$$G_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 G_2(z) - \pi ic(cz+d)$$

This equation shows the **failure** of G_2 to transform like a modular form of weight 2.

Proofs and detailed discussion can be found in:

- N. Koblitz: *Introduction to Elliptic Curves and Modular Forms*, GTM 97, Springer, 1993.
- D. Zagier: *Elliptic Modular Forms and Their Applications*, in “The 1-2-3 of Modular Forms”, Springer, 2008. Available online: http://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/978-3-540-74119-0_1/fulltext.pdf

Normalized Eisenstein Series

For even integers $k \geq 2$, we define the *normalized Eisenstein series*:

$$E_k(z) := \frac{1}{\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where B_k is the k -th Bernoulli number (appears when expressing $\zeta(k)$).

This normalization ensures that $E_k(z) \in \mathbb{Q}[[q]]$, with rational Fourier coefficients.

Motivation

Modular forms appear in many areas of mathematics, with applications ranging from number theory to cryptography.

Let us begin with a classical result from number theory:

Theorem 2 (Lagrange, 1770)

Every positive integer can be expressed as a sum of four squares.

Examples:

$$1 = 1^2 + 0^2 + 0^2 + 0^2,$$

$$30 = 1^2 + 2^2 + 3^2 + 4^2 = 0^2 + 1^2 + 2^2 + 5^2,$$

$$2025 = 26^2 + 25^2 + 20^2 + 18^2 = 26^2 + 24^2 + 22^2 + 17^2 = 26^2 + 26^2 + 23^2 + 12^2 = \dots$$

Note: This decomposition is not unique.

Counting Representations

Question: In how many ways can a natural number n be written as a sum of four squares?

We define the function:

$$r_4(n) := \#\{(a, b, c, d) \in \mathbb{Z}^4 \mid n = a^2 + b^2 + c^2 + d^2\}$$

This question was answered explicitly by Jacobi:

Theorem 3 (Jacobi's four-square theorem, 1834)

For all $n \in \mathbb{Z}_{\geq 1}$, we have:

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d$$

Example 1: If p is prime, then $r_4(p) = 8(p + 1)$.

Example 2: The positive divisors of 2025 are 1, 3, 5, 9, 15, 25, 27, 45, 75, 81, 135, 225, 405, 675, 2025 (none divisible by 4), hence:

$$r_4(2025) = 8(1 + 3 + 5 + \cdots + 2025) = 30008$$

Generating Series and Modular Forms

To prove such theorems, we consider the generating series:

$$F(q) = \sum_{n \geq 0} r_4(n)q^n = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + \dots$$

It turns out that $F(q)$ is a modular form of weight 2 and level 4. Spoiler: the space of modular forms of weight 2 and level 4 has dimension 2. It is spanned by Eisenstein series:

$$E_2(q) - 2E_2(q^2), \quad E_2(q) - 4E_2(q^4)$$

Using analytic methods, one can show:

$$F(q) = -\frac{1}{3} (E_2(q) - 4E_2(q^4))$$

This identity implies Jacobi's theorem.

Divisor Sums and Eisenstein Series

Definition 4

For $\ell \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$, define:

$$\sigma_\ell(n) := \sum_{d|n} d^\ell$$

Examples:

$$\sigma_0(6) = 4, \quad \sigma_1(6) = 12 \quad (\text{divisors: } 1, 2, 3, 6)$$

More values:

n	$\sigma_1(n)$	$\sigma_3(n)$	$\sigma_5(n)$	$\sigma_7(n)$	$\sigma_9(n)$	$\sigma_{11}(n)$
1	1	1	1	1	1	1
2	3	9	33	129	513	2049
3	4	28	244	2188	19684	177148
4	7	73	1057	16513	262657	4196353
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots

Eisenstein Series

We define Eisenstein series via their q -expansions:

$$E_2(z) = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q^n$$

$$E_4(z) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$$

$$E_6(z) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n$$

$$E_8(z) = 1 + 480 \sum_{n \geq 1} \sigma_7(n) q^n$$

Note: The constants arise from normalizations.

An Identity Among Eisenstein Series

The space of modular forms is a graded ring.

Observation: Both E_8 and E_4^2 are modular forms of weight 8 and start with $1 + \dots$, and the space of weight 8 modular forms has dimension 1, so:

$$E_8(q) = E_4(q)^2$$

Taking the q^n coefficients yields:

Theorem 5 (Hurwitz Identity)

For all $n \geq 1$,

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

Example: For $n = 3$:

$$\sigma_7(3) = 2188 = \sigma_3(3) + 120(\sigma_3(1)\sigma_3(2) + \sigma_3(2)\sigma_3(1)) = 28 + 120 \cdot 18$$

Differentiating Modular Forms

Modular forms are holomorphic, so we can differentiate them with respect to τ .

Given a modular form $f(z) = \sum_{n=0}^{\infty} a_n q^n$, we define:

$$f' := \frac{1}{2\pi i} \frac{d}{dz} f = q \frac{d}{dq} f = \sum_{n=1}^{\infty} n a_n q^n$$

The factor $\frac{1}{2\pi i}$ ensures rationality of the Fourier coefficients.

However: The derivative f' is generally *not* a modular form!

Failure of Modularity of the Derivative

Proposition 6

Let $f \in M_k$. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have:

$$f' \left(\frac{az + b}{cz + d} \right) = (cz + d)^{k+2} f'(z) + \frac{k}{2\pi i} c (cz + d)^{k+1} f(z)$$

Proof: Exercise.

The Serre Derivative

Definition 7 (Serre derivative)

Let $f \in M_k$. The Serre derivative is defined as:

$$\partial_k f := f' - \frac{k}{12} E_2 f$$

Proposition 8

If $f \in M_k$, then $\partial_k f \in M_{k+2}$.

Idea of proof: Use the transformation law of E_2 :

$$E_2 \left(\frac{az + b}{cz + d} \right) = (cz + d)^2 E_2(z) - \frac{6}{\pi i} c(c\tau + d)$$

Quasimodular Forms

Definition 9

The ring of **quasimodular forms** is defined by:

$$\mathcal{M} := \mathbb{C}[E_2, E_4, E_6]$$

Proposition 10

The ring \mathcal{M} is closed under differentiation. In particular:

$$\begin{aligned} E_2' &= \frac{E_2^2 - E_4}{12} & E_4' &= \frac{E_2 E_4 - E_6}{3} \\ E_6' &= \frac{E_2 E_6 - E_4^2}{2} \end{aligned}$$

Relations Among Fourier Coefficients

Modular forms of the same weight lie in finite-dimensional spaces.
This implies that identities such as:

$$E_8 = E_4^2 \quad \text{and} \quad E_{10} = E_4 E_6$$

lead to relations among divisor sums, e.g.:

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

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

These also yield congruences such as:

$$11\sigma_9(n) \equiv 21\sigma_5(n) - 10\sigma_3(n) \pmod{5040}$$

Derivatives and Further Identities

Using the formula:

$$E_2'(z) = -24 \sum_{n=1}^{\infty} n\sigma_1(n)q^n$$

and the first equation in Proposition 10, we obtain:

$$6n\sigma_1(n) = 5\sigma_3(n) + \sigma_1(n) - 12 \sum_{j=1}^{n-1} \sigma_1(j)\sigma_1(n-j)$$

This is another non-trivial identity among divisor sums.

Ramanujan's Tau Function and Congruences

Proposition 11

① We have:

$$\Delta(z) = \frac{691}{65520} E_{12} - \frac{691}{156} \left(\frac{1}{720} E_4^3 - \frac{1}{1008} E_6^2 \right)$$

② For all $n \geq 1$:

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

This follows from the fact that E_4^3 and E_6^2 span M_{12} , and by comparing the Fourier coefficients of:

$$E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n$$

Modular Forms of Higher Level

Until now, we considered modular forms for the full modular group $SL_2(\mathbb{Z})$, i.e., level 1.

Definition 12 (Congruence Subgroups)

For $N \geq 1$, define:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) = \{ \gamma \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N} \}$$

$$\Gamma(N) = \{ \gamma \in \Gamma_1(N) : b \equiv 0 \pmod{N} \}$$

A subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ is called **congruence subgroup** if there exists a N with $\Gamma(N) \subseteq \Gamma$. The smallest such N is called the **level** of Γ .

We have inclusions:

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z})$$

The Slash Operator

Definition 13

Let $f : H \rightarrow \mathbb{C}$ be a function, $k \in \mathbb{Z}$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. The **slash operator of weight k** is defined by:

$$(f|_k\gamma)(z) := (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right)$$

This defines a right action of the group $\mathrm{SL}_2(\mathbb{Z})$ on the space of holomorphic functions on the upper half-plane.

Remark. If $f \in \mathcal{O}(H)$, then $f|_k\gamma \in \mathcal{O}(H)$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Remark. If f is a **modular form** then $f|_k\gamma = f$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Exercise 1

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $z \in H$, and $f \in \mathcal{O}(H)$. Define:

$$\gamma(z) := \frac{az + b}{cz + d}, \quad (f|_k\gamma)(z) := (cz + d)^{-k} f(\gamma(z))$$

- 1 Verify that $\mathrm{SL}_2(\mathbb{Z})$ acts on H from the left:

$$\gamma'(\gamma(z)) = (\gamma'\gamma)(z), \quad \mathrm{Id}(z) = z$$

- 2 Show that the slash operator defines a right action on $\mathcal{O}(H)$, i.e.:

$$f|_k\mathrm{Id} = f, \quad (f|_k\gamma')|_k\gamma = f|_k(\gamma' \cdot \gamma)$$

for all $f \in \mathcal{O}(H)$, $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$.

Modular Forms for Subgroups

Definition 14 (Modular form)

Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $k \in \mathbb{Z}$. A function $f : H \rightarrow \mathbb{C}$ is a **modular form** of weight k for Γ if:

- 1 $f|_k \gamma = f \quad \forall \gamma \in \Gamma$
- 2 $f|_k \gamma$ is holomorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$

We denote this space by $M_k(\Gamma)$. When $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, this recovers the usual space M_k .

Example: Level 4 and Weight 2

Lemma 15

① For all $N > 0$, define:

$$G_{2,N}(z) := G_2(z) - NG_2(Nz) \in M_2(\Gamma_0(N))$$

② $\Gamma_0(4)$ is generated by $\pm T$ and $\pm \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$

③ $\dim_{\mathbb{C}} M_2(\Gamma_0(4)) = 2$

Reference: Diamond–Shurman, Theorem 3.5.1 and Exercise 1.2.4

Theta Function and the Four-Square Theorem

We define the theta function:

$$\Theta(z) := \sum_{n \in \mathbb{Z}} q^{n^2}$$

It satisfies two functional equations:

$$\Theta(z+1) = \Theta(z), \quad \Theta\left(-\frac{1}{4z}\right) = \sqrt{2z/i} \Theta(z)$$

Define:

$$F(q) := \sum_{n=0}^{\infty} r_4(n) q^n$$

We observe:

$$F(q) = \Theta(z)^4$$

Modularity of Θ^4

Corollary 16

$$\Theta^4(z) \in M_2(\Gamma_0(4))$$

Idea of proof:

- Use the generators of $\Gamma_0(4)$
- Check transformation formulas using Poisson summation
- Conclude using Lemma 15 and modularity of Θ

Proof of Jacobi's Four-Square Theorem

Recall:

$$F(q) = \sum_{n \geq 0} r_4(n)q^n = \Theta^4(z)$$

We know:

$$\dim M_2(\Gamma_0(4)) = 2 \quad \text{and} \quad G_{2,2}, G_{2,4} \text{ form a basis}$$

Compare first two Fourier coefficients of Θ^4 and $G_{2,4}$, one finds:

$$\Theta^4(z) = -\frac{1}{\pi^2} G_{2,4}(z)$$

This gives the explicit formula for $r_4(n)$, as stated in Theorem 3.

Hecke Operators on Modular Forms of Level 1

Let $k \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$. We define the n -th Hecke operator T_n acting on modular forms of weight k .

Definition: Let

$$X_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}) \mid a \geq 1, ad = n, 0 \leq b < d \right\}.$$

The n -th Hecke operator is defined by:

$$T_n(f)(z) := \sum_{\gamma \in X_n} \det(\gamma)^{k-1} (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

Remark: The action is compatible with the right action of $\text{SL}_2(\mathbb{Z})$:

$$(T_n f)|_k \gamma = T_n(f|_k \gamma).$$

Properties of Hecke Operators

Proposition 17

Let f be a modular form of weight k . Then:

- $T_n(f)$ is again a modular form of weight k
- T_n preserves the space M_k and S_k

Proposition 18 (Multiplicative relations:)

For all $m, n \geq 1$:

- If $\gcd(m, n) = 1$, then $T_m T_n = T_{mn}$
- If p is prime, then:

$$T_{p^n} = T_p T_{p^{n-1}} - p^{k-1} T_{p^{n-2}}$$

Proposition 19 (Fourier formula)

Let $f(\tau) = \sum_{m \geq 0} a_m q^m$, then:

$$T_n(f)(z) = \sum_{m \geq 0} \left(\sum_{d | \gcd(m, n)} d^{k-1} a_{mn/d^2} \right) q^m.$$

In particular:

$$T_p(f)(z) = \sum_{m \geq 0} (a_{mp} + p^{k-1} a_{m/p}) q^m \quad (\text{with } a_{m/p} = 0 \text{ if } p \nmid m)$$

Example 1

$$E_4(z) = 1 + 240q + 2160q^2 + \dots$$

- $T_2(E_4) = (1 + 2^3)E_4 = 9E_4$
- *In general:* $T_n(E_k) = \sigma_{k-1}(n)E_k$

Example 2

$$\Delta(z) = q - 24q^2 + 252q^3 - \dots$$

- Δ is a cusp form of weight 12
- $T_n(\Delta) = \tau(n)\Delta$ with $\tau(n)$ the Ramanujan tau function
- $\tau(nm) = \tau(n)\tau(m)$ if $\gcd(n, m) = 1$

Conclusion: Modular forms that are eigenvectors for all T_n have arithmetic significance. They are called **Hecke eigenforms**.

Maeda's Conjecture on Hecke Operators

Conjecture 1 (Maeda)

Let $k \geq 12$ be an even integer. Then:

- The characteristic polynomial of the Hecke operator T_n (typically T_2) acting on the cusp form space S_k of level 1 and weight k is *irreducible over* \mathbb{Q} .
- Its Galois group is the full symmetric group \mathfrak{S}_d , where $d = \dim S_k$.

Significance:

- Suggests deep arithmetic and algebraic structure of Hecke eigenforms.
- Implies strong interdependence among the Fourier coefficients of cusp forms.
- Verified computationally for many weights k .

Elliptic Curves, Galois Representations, and Hecke Operators

Hecke eigenforms of weight 2 correspond to **elliptic curves** over \mathbb{Q} :

- Thanks to the Modularity Theorem (formerly the Taniyama-Shimura conjecture) by Wiles, Taylor et al.
- Fourier coefficients a_p of an eigenform $f \in S_2(\Gamma_0(N))$ give the trace of Frobenius of a corresponding elliptic curve modulo p .

Galois representations:

- To each eigenform f , we can attach a continuous Galois representation:

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Q}_\ell)$$

such that $\text{Tr}(\rho_f(\text{Frob}_p)) = a_p$.

- These representations are essential in modern number theory (e.g. proof of Fermat's Last Theorem).

Newforms at Level 35, Weight 2

The space $S_2(\Gamma_0(35))$ contains two Galois-inequivalent newforms:

Rational newform f_1 :

$$f_1(q) = q + q^3 - 2q^4 - q^5 + q^7 - 2q^9 + \dots$$

Hecke field: \mathbb{Q}

Corresponds to the elliptic curve 35.a1 (LMFDB label).

Quadratic newform f_2 :

$$f_2(q) = q - \beta q^2 + (\beta - 1)q^3 + (\beta + 2)q^4 + q^5 - 4q^6 + \dots \quad \text{with } \beta = \frac{(1 + \sqrt{17})}{2}$$

Hecke field: $\mathbb{Q}(\sqrt{17})$

Takeaway: This example illustrates that different newforms at the same level and weight can have distinct Hecke fields, with one corresponding to an elliptic curve over \mathbb{Q} , and the other to a simple abelian surface with real multiplication.

Further Reading and References

- Serre, J. P., *A course in Arithmetic*, Springer (1973)
- Diamond, Shurman: *A First Course in Modular Forms* (GTM 228)
- Koblitz: *Introduction to Elliptic Curves and Modular Forms* (GTM 97)
- Zagier: *Elliptic Modular Forms and their Applications*, in "The 1-2-3 of Modular Forms"
- Kilford, Freitag–Busam, Serre, Stein–Shakarchi, Lang ...

See Zagier's chapter online: http://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/978-3-540-74119-0_1/fulltext.pdf