

**R.E.U. IN NUMBER THEORY: INVESTIGATING  
ELLIPTIC CURVES, MODULAR FORMS AND  $q$ -SERIES**

Brief Project Descriptions

I. Research on Elliptic Curves and Modular Forms.

Team I will study the arithmetic properties of modular forms. We shall assume familiarity with undergraduate Complex Analysis. Modular forms play a central role in the proof of Fermat's Last Theorem. Although it would be exciting to lead students in these directions, such a task would be far too ambitious for a seven week summer program. Nevertheless, we will have no difficulty introducing some of the deeper properties of modular forms, along with their connections to the arithmetic of elliptic curves.

Here we shall focus on the connection between elliptic curves and modular forms and orthogonal polynomials defined using certain *bizarre* scalar products which have only recently been discovered.

Team I will study the arithmetic captured by the modular  $j$ -function

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^3 + \dots$$

They will be assigned the project of studying scalar products on the polynomial ring

$$V = \mathbb{R}[j].$$

Here we briefly describe the scalar products which will be considered by Team I. If  $\Psi \in V$ , then we define the product  $(\cdot, \cdot)_{\Psi}$  on  $V$  by

$$(f, g)_{\Psi} := \int_{\pi/3}^{\pi/2} f(e^{i\theta})g(e^{i\theta})\Psi(e^{i\theta})d\theta.$$

Although  $f, g$  and  $\Psi$  are polynomials in  $j$ , here they are viewed as modular functions (i.e. we view  $j$  as  $j(z)$ ).

If the scalar product is non-degenerate, then one may define a sequence of *orthogonal polynomials* with respect to  $\Psi$ , say  $P_{0,\Psi}, P_{1,\Psi}, \dots \in V$ . These polynomials are defined by letting  $P_{0,\Psi}(j) = 1$ , and by recursively defining the others by the Gram-Schmidt formula

$$P_{n,\Psi} := j^n - \sum_{m=0}^{n-1} \frac{(j^n, P_{m,\Psi})_{\Psi}}{(P_{m,\Psi}, P_{m,\Psi})_{\Psi}} \cdot P_{m,\Psi}.$$

Typeset by  $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX

The general theory of orthogonal polynomials has a long history with deep connections to many areas of Mathematics. However, the products defined above have not been studied as extensively.

In an important recent paper, M. Kaneko and D. Zagier considered these products in the case  $\Psi = 1$  (a case previously considered by A. O. L. Atkin in unpublished work). Although the calculation is not straightforward, it turns out that the first few orthogonal polynomials with respect to  $\Psi$  are:

$$\begin{aligned} P_{0,1}(j) &= 1, \\ P_{1,1}(j) &= j - 720, \\ P_{2,1}(j) &= j^2 - 1640j + 269280, \\ P_{3,1}(j) &= j^3 - 12567j^2/5 + 1526958j - 107765856. \end{aligned}$$

Atkin, Kaneko and Zagier proved a striking property satisfied by these polynomials in connection with the theory of elliptic curves.

The isomorphism class of an elliptic curve  $E$  in an algebraically closed field is dictated by its  $j$ -invariant  $j(E)$ . Here we concern ourselves, for primes  $p$ , the polynomials

$$S_p(j) := \prod_{E/\overline{\mathbb{F}}_p \text{ supersingular}} (j - j(E)).$$

Here  $\overline{\mathbb{F}}_p$  denotes the algebraic closure of the finite field with  $p$  elements, and the product is over isomorphism classes of supersingular elliptic curves (note: an elliptic curve is supersingular in  $\overline{\mathbb{F}}_p$  if its group of rational points does not contain a torsion point of order  $p$ ). Atkin, Kaneko and Zagier proved the following theorem regarding the connection between the supersingular loci  $S_p(j)$  and the orthogonal polynomials  $P_{n,1}$ .

**Theorem.** *If  $p \geq 5$  is prime and  $g_p$  denotes the number of supersingular  $j$ -invariants in characteristic  $p$ , then*

$$P_{g_p,1} \equiv S_p(x) \pmod{p}.$$

This result provides a deep connection between two completely different sets of objects. Team I will be assigned, among other projects, the task of generalizing this result for more general  $\Psi$ .

## II. Research on $q$ -series, Partitions and Zeta-values.

Team II will study the arithmetic of partitions and  $q$ -series. We shall assume familiarity with elementary Combinatorics and Complex Analysis. To motivate this research project, we begin by recalling Euler's celebrated *Pentagonal Number Theorem*:

$$\prod_{n=1}^{\infty} (1 - q^n) = \sum_{k=-\infty}^{\infty} (-1)^k q^{(3k^2+k)/2}.$$

This identity has a simple combinatorial interpretation in terms of partitions. Recall that a partition of an integer  $n$  is any non-increasing sequence of positive integers with sum  $n$ . In terms of partitions, this identity implies that the number of partitions of an integer  $n$  into an even number of distinct parts equals the number of partitions of  $n$  into an odd number of distinct parts, unless  $n$  is of the form  $(3k^2 + k)/2$ . For example, observe that the partitions of  $n = 6$  into distinct parts are:

$$\begin{aligned} &6, & 3 + 2 + 1, \\ &5 + 1, & 4 + 2. \end{aligned}$$

There are four partitions of 6 into distinct parts, and they are equally divided into those partitions with an even number as well as those with an odd number of parts.

In a recent paper, Zagier proved the following  $q$ -series identity (note. empty products equal 1 throughout):

$$\sum_{n=0}^{\infty} \left( q \prod_{n=1}^{\infty} (1 - q^{24n}) - q(1 - q^{24})(1 - q^{48}) \cdots (1 - q^{24n}) \right) = q \prod_{n=1}^{\infty} (1 - q^{24n}) \cdot D(q) + E(q).$$

Here the series  $D(q)$  and  $E(q)$  are defined by

$$\begin{aligned} D(q) &= -\frac{1}{2} + \sum_{n=1}^{\infty} \frac{q^{24n}}{1 - q^{24n}} = -\frac{1}{2} + \sum_{n=1}^{\infty} d(n)q^{24n} = -\frac{1}{2} + q^{24} + 2q^{48} + 2q^{72} + 3q^{96} + \dots, \\ E(q) &= \frac{1}{2} \sum_{n=1}^{\infty} \left( \frac{12}{n} \right) nq^{n^2} = \frac{1}{2}q - \frac{5}{2}q^{25} - \frac{7}{2}q^{49} + \frac{11}{2}q^{121} + \dots \end{aligned}$$

Here  $d(n)$  denotes the number of positive divisors of  $n$ , and

$$\left( \frac{12}{n} \right) := \begin{cases} 1 & \text{if } n \equiv 1, 11 \pmod{12}, \\ -1 & \text{if } n \equiv 5, 7 \pmod{12}, \\ 0 & \text{otherwise.} \end{cases}$$

This identity is indeed a *strange identity* which may be viewed as the “summing of the tails” of the identity in Euler’s Pentagonal Number Theorem.

Zagier’s identity may be viewed as a special case of a general phenomenon: classical  $q$ -series identities have a “sum of tails” form. In a surprising finding, Zagier observed that his identity implies a generalization of the classical fact that

$$\frac{t}{e^t - 1} = 1 + \sum_{n=1}^{\infty} (-1)^{n+1} \zeta(1 - n) \cdot \frac{t^n}{(n - 1)!},$$

where  $\zeta(s)$  is the Riemann zeta-function. In this direction, Zagier used his identity to show that

$$-e^{-t/24} \sum_{n=0}^{\infty} (1 - e^{-t})(1 - e^{-2t}) \cdots (1 - e^{-nt}) = \frac{1}{2} \sum_{n=0}^{\infty} (-1/24)^n \cdot L(\chi_{12}, -2n - 1) \cdot \frac{t^n}{n!},$$

where  $\chi_{12} = \binom{12}{n}$ . In a nutshell, plugging in  $q = e^{-t}$  into the identity and expanding as a power series in  $t$  using the Taylor expansion

$$e^{-t} = 1 - t + \frac{1}{2}t^2 - \frac{1}{6}t^3 + \frac{1}{24}t^4 - \dots$$

produces values of  $L$ -functions.

In view of Zagier's peculiar result, it is natural to seek a more general theory which uses the combinatorics of  $q$ -series and partitions to produce further generating functions whose coefficients are the values of  $L$ -functions and  $\zeta$ -functions. Team II will consider further questions in this direction.