UNIVERSITY of HAWAIʻI at MĀNOA

Submitted In Partial Fulfillment Of The Plan B Requirements For The Degree of Master of Arts In Mathematics

A MODULAR FORMS APPROACH TO ARITHMETIC CONVOLUTED IDENTITIES

ABSTRACT. In 2004, H. Farkas found a series of identities which relate the convolution of a certain arithmetic function with an analogue of the classical σ-function. In 2009, P. Guerzhoy and W. Raji interpreted series of identities of this kind using generating functions and modular forms. Their results pertain to primes $p \equiv 3 \mod 4$. In this paper, we address the primes $p \equiv 5 \mod 8$ and obtain four new series of similar identities. Our methods are close to those employed by Guerzhoy and Raji.

Author: Christina Mende
Master's Committee:
Pavel Guerzhoy
Michelle Manes

Graduate Committee:
Ralph Freese
George Wilkens
David Yuen

0. Acknowledgments

Thank you to my advisor Dr. Guerzhoy for his endless patience, understanding, and most of all for his support. I would not have gotten this far without his knowledge and help.

Thanks also to Dr. Manes for taking time out of her busy schedule and giving me feedback on my paper.

I would also like to thank everyone in the Math Division office, especially Sue and Alicia for their hard work and dedication.

Finally, I would like to thank my friends and especially my family for their encouragement and support even when things seemed impossible.

Contents

1. Motivation

For a prime $p \equiv 3 \mod 4$, let

$$\delta_p(n) = \sum_{d|n} \left(\frac{-p}{d}\right) \tag{1}$$

which is the difference between the numbers of those (positive) divisors of n which are quadratic residues and non-residues modulo p. In 2004, H. Farkas in [3] found an elegant identity related to the convolution of the arithmetic function $\delta_3(n)$:

$$\delta_3(n) + 3\sum_{j=1}^{n-1} \delta_3(j)\delta_3(n-j) = \sigma_3'(n) \tag{2}$$

for $n \geq 1$, where

$$\sigma_3'(n) = \sum_{\substack{d|n \\ 3\nmid d}} d \tag{3}$$

In 2009, Guerzhoy and Raji in [2] gave a modular interpretation of this identity using generating functions. Specifically, they interpreted this as an identity between two modular forms. This interpretation allowed these authors to find a similar identity for $p = 7$. Furthermore, they proved the absence of "similar" identities in a certain strict sense, as well as abundance of "similar" identities when the "similarity" condition is slightly relaxed. The latter claim has been recently illustrated by K. Williams in [8], where a list of twelve "similar" identities is proved by the means of elementary combinatorics. Note that all quadratic characters under consideration both in [2] and [8] are odd, therefore appearance of only primes $p \equiv 3 \mod 4$ (see Example 2 below). In this paper, we make an attempt to fill in this gap.

It is mentioned in [2] and can be seen in [8] that the further one goes the more complicated (and perhaps less interesting) these identities become, though their "form", at least from the viewpoint taken in [2], remains unaltered. Loosely speaking, if we consider properly arranged generating functions, the identities may be expressed as those between modular forms of weight two. Most of these modular forms are either Eisenstein series of weight two, or products of Eisenstein series of weight one.

The goal of this paper is to revise the modular approach taken in [2] to identities of this kind and to find and prove new examples which are closer by their simplicity and elegance to the original identity (2) of Farkas (and its analog for $p = 7$ from [2]).

Our principal idea is to take into consideration only quadratic characters. In order to formulate our main result, we will need some notation related to Dirichlet characters. We devote the next section to this discussion.

2. Dirichlet characters

Let $N > 1$ be an integer. By definition, a Dirichlet character φ modulo N is a group homomorphism

$$\varphi\ : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*,$$

where $\mathbb{C}^*$ is the set of complex numbers without zero considered as a multiplicative group. For a Dirichlet character φ we will denote by the same letter (and also call it a Dirichlet character) the map

$$\varphi\ : \mathbb{Z} \to \mathbb{C}$$

obtained as the composition of φ with the natural projection

$$\pi\ :\ \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z},$$

and by letting $\varphi(n) = 0$ if $\gcd(n, N) \neq 1$.

It is convention to call the Dirichlet character corresponding to the trivial character of $(\mathbb{Z}/N\mathbb{Z})^*$ the *trivial character modulo* N. For the case when $N = 1$, we call the trivial character the *principal character* and denote it as χ_0.

The concept of even and odd characters mentioned before is as follows: If $\varphi(-1) = 1$ then φ is called *even*. If $\varphi(-1) = -1$ then the character φ is called *odd*.

If χ is a Dirichlet character modulo N and $\chi^2(n) = \chi(n)\chi(n) = 1$ for all $n \in \mathbb{Z}$ with $(n, N) = 1$ then we call χ a *quadratic character*. Similarly, if $\chi^4(n) = 1$ for all $n \in \mathbb{Z}$ with $(n, N) = 1$ then we call χ a *quartic character*.

Proposition 1. *Let φ be a Dirichlet character modulo N. Its image is a subset of roots of unity of degree $\phi(N)$, where ϕ is Euler's ϕ-function. If N is a prime, then the character φ is defined uniquely by its value $\varphi(g)$, where g is a generator of $(\mathbb{Z}/N\mathbb{Z})^*$.*

Proof. Since $(\mathbb{Z}/N\mathbb{Z})^*$ is finite with order $\phi(N)$ we have that for each $a \in (\mathbb{Z}/N\mathbb{Z})^*$,

$$a^{\phi(N)} = 1.$$

By definition, φ is a homomorphism, so using the above we can easily show that its image must be a subset of roots of unity of degree $\phi(N)$.

Now, if N is a prime then $\mathbb{Z}/N\mathbb{Z}$ is a finite field, and $(\mathbb{Z}/N\mathbb{Z})^*$ is the multiplicative group of nonzero units of this field. Hence, there exists a g such that

$$\langle g \rangle = (\mathbb{Z}/N\mathbb{Z})^*.$$

So any element of $(\mathbb{Z}/N\mathbb{Z})^*$ may be written in the form g^k where $k \in \mathbb{Z}$. Thus since

$$\varphi(g^k) = \varphi^k(g),$$

we see that φ is defined uniquely by $\varphi(g)$.

$\square$

We now look at two particular Dirichlet characters whose definitions are taken from [6, pp. 82–83].

Example. **Legendre and Kronecker symbols**

Let p be an odd prime number. Then for $n \in \mathbb{Z}$, we put

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv n \mod p \text{ is solvable in } \mathbb{Z}, \\ -1 & \text{if } x^2 \equiv n \mod p \text{ is unsolvable in } \mathbb{Z}, \\ 0 & \text{if } p|n. \end{cases}$$

This is known as the *Legendre symbol*. We note that the mapping "$n \mapsto \left(\frac{n}{p}\right)$" is a Dirichlet character mod p [6, pp. 82].

Going further, we define $\left(\frac{a}{b}\right)$ for $a, b \in \mathbb{Z}$ and $(a, b) \neq (0, 0)$ in the following manner:

For b an odd prime, we let $\left(\frac{a}{b}\right)$ as above.

If $b = 2, \pm 1$, or 0 then

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \mod 8, \\ -1 & \text{if } a \equiv 5 \mod 8, \\ 0 & \text{otherwise}, \end{cases}$$

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0, \\ -1 & \text{if } a < 0, \end{cases}$$

$$\left(\frac{a}{1}\right) = 1,$$

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & \text{if } a = 1, \\ 0 & \text{if } a \neq 1. \end{cases}$$

Finally, let $b \in \mathbb{Z} \setminus \{0\}$ and write is as a product of ± 1 and prime numbers

$$b = \epsilon \prod p \quad \text{where } \epsilon = \pm 1 \text{ and } p \text{ prime}.$$

Define

$$\left(\frac{a}{b}\right) = \left(\frac{a}{\epsilon}\right) \prod_p \left(\frac{a}{p}\right).$$

This generalization is callled the *Kronecker symbol*. It is known that for any $d \in \mathbb{Z} \setminus \{0\}$, the mapping "$n \mapsto \left(\frac{d}{n}\right)$" is a Dirichlet character; furthermore if d is a square-free integer except possibly $d \equiv 0 \mod 4$ or $d \equiv 1 \mod 4$ then the mapping is actually a Dirichlet character modulo $|d|$[6, pp. 83,84].

As mentioned previously, [2] and [8] considered only odd quadratic characters with primes $p \equiv 3 \mod 4$. We now take into consideration even quadratic characters with those primes $p \equiv 1 \mod 4$. Notice that by construction,

$$\left(\frac{p}{-1}\right) = \operatorname{sign}(p).$$

In particular, we have that

$$\left(\frac{5}{-1}\right) = \left(\frac{13}{-1}\right) = 1,$$

which shows that for $p = 5$ or 13 the Kronecker symbol is an even Dirichlet character.

A well-known fact, is that the Kronecker symbol is a nontrivial, quadratic character. In this way, we can describe the Kronecker symbol as the quadratic character which sends a generator $g \in (\mathbb{Z}/p\mathbb{Z})^*$ to $-1 \in \mathbb{C}$.

We now consider the following proposition.

Proposition 2. *Let p be a prime, and let $\zeta \in \mathbb{C}$ satisfy*

$$\zeta^{p-1} = 1.$$

Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. There exists a unique Dirichlet character φ modulo p such that

$$\varphi(g) = \zeta.$$

Proof. Define the mapping

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^* \text{ by } g^k \mapsto \zeta^k \text{ where } k \in \mathbb{Z}.$$

To see that φ is a well-defined, suppose that $g^{k_1} = g^{k_2}$. Then $k_1 \equiv k_2 \mod p-1$.

Since $\zeta^{p-1} = 1$, we can conclude that

$$\frac{\zeta^{k_1}}{\zeta^{k_2}} = \zeta^{k_1 - k_2} = 1.$$

Thus, $\varphi(g^{k_1}) = \varphi(g^{k_2})$ when $g^{k_1} = g^{k_2}$ and so the mapping is well-defined.

By construction, φ is defined under multiplication, thus it is easy to see that φ is, in fact, a homomorphism. Thus we can conclude φ is a Dirichlet character modulo p. Uniqueness then follows from Proposition 1. $\square$

For a Dirichlet character φ, we define $\overline{\varphi}$ by

$$\overline{\varphi}(n) = \overline{\varphi(n)}$$

for any $n \in \mathbb{Z}$, where the bar denotes the complex conjugation. It is easy to check that $\overline{\varphi}$ is again a Dirichlet character. Clearly, a product (as $\mathbb{C}$-valued functions on $\mathbb{Z}$) of two Dirichlet characters is again a Dirichlet character, in particular, the square of a Dirichlet character is also a Dirichlet character. The above proposition allows us, in some cases, to find a square root of the Kronecker symbol.

Proposition 3. *Let p be a prime such that*

$$p \equiv 1 \mod 4.$$

There exist exactly two Dirichlet characters χ and $\overline{\chi}$ modulo p such that for any $n \in \mathbb{Z}$,

$$\chi^2(n) = \overline{\chi}^2(n) = \left(\frac{p}{n}\right).$$

Proof. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. By our choice of p, we know that $\left(\frac{p}{n}\right)$ is a Dirichlet character modulo p.

As noted previously, we can describe $\left(\frac{p}{n}\right)$ as the Dirichlet character which sends g to -1. Thus, to find a "square root" of the Kronecker symbol, we have exactly two choices: $g \mapsto i$ or $g \mapsto -i$.

Without loss of generality, choose, $i \in \mathbb{C}^*$, then since $p \equiv 1 \mod 4$ we have that $i^{p-1} = 1$. By Proposition 2, there exists a unique Dirichlet character, call it χ such that $\chi(g) = i$. So taking $\overline{\chi}$ as the other Dirichlet character, we have that

$$\chi^2(g) = \overline{\chi}^2(g) = -1.$$

By Proposition 1, we know that for prime p, Dirichlet characters are uniquely determined by the image of its generator. Hence it must be that $\chi^2(n) = \overline{\chi}^2(n) = \left(\frac{p}{n}\right)$ for all n. □

We also will need the definition of generalized Bernoulli numbers. The generalization is related to Dirichlet characters. Let ψ be a Dirichlet character modulo N. Generalized Bernoulli numbers $B_{n,\psi}$ are defined as the Taylor series coefficients of the function in t:

$$\sum_{a=1}^{N} \psi(a) \frac{te^{at}}{e^{Nt}-1} = \sum_{n=0}^{\infty} B_{n,\psi} \frac{t^n}{n!}.$$

Here we take note of the similarity to the classical Bernoulli numbers:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

3. Principal results

In order to state our results, we need to introduce some more notation. In this section, p is a prime such that $p \equiv 5 \mod 8$. We let φ_p be the *trivial* character modulo p, namely the Dirichlet character defined by

$$\varphi_p(n) = \begin{cases} 1 & \text{if } p \nmid n \\ 0 & \text{otherwise.} \end{cases}$$

Denote by χ_p a Dirichlet character modulo p such that

$$\chi_p^2(n) = \left(\frac{p}{n}\right).$$

This Dirichlet character is defined up to complex conjugation due to Proposition 3. More precisely, in the cases when $p = 5$ or $p = 13$ we let χ_p be the unique Dirichlet character using the requirement

$$\chi_p(2) = i.$$

This requirement defines χ_p because $2 \mod p$ is a generator of both $(\mathbb{Z}/5\mathbb{Z})^*$ and $(\mathbb{Z}/13\mathbb{Z})^*$.

We let

$$\delta_p(n) = \sum_{0<d|n} \chi_p(n/d) = \sum_{0<d|n} \chi_p(d),$$

and emphasize its similarity with (1).

We also define

$$\sigma'_p(n) = \sum_{0<d|n} \varphi_p(d)d = \sum_{\substack{0<d|n \\ p\nmid d}} d,$$

and emphasize its similarity with (3).

The following result is now a complete analogue of Farkas' identity. Following the convention of notation with complex numbers, a bar denotes complex conjugation, and $\Re(z)$ (resp. $\Im(z)$) denotes the real (resp. imaginary) part of a complex number z.

Theorem 1. *Let p be 5 or 13. For any integer $n \geq 1$,*

$$\Re\left(\beta_p \delta_p(n)\right) + \alpha_p \sum_{k=1}^{n-1} \delta_p(k)\overline{\delta_p(n-k)} = \sigma'_p(n),$$

where

$$\alpha_p = \begin{cases} 5/3 & \text{if } p = 5, \\ 1 & \text{if } p = 13, \end{cases}$$

and

$$\beta_p = \begin{cases} (3-i)/3 & \text{if } p = 5, \\ 1-i & \text{if } p = 13. \end{cases}$$

Our consideration of quartic Dirichlet characters instead of just quadratic characters provides some additional freedom. Namely, instead of the convolution

$$\sum_{k=1}^{n-1} \delta_p(k)\overline{\delta_p(n-k)}$$

we may also consider the convolution

$$\sum_{k=1}^{n-1} \delta_p(k)\delta_p(n-k)$$

and expect to produce similar identities. Our next theorem confirms this expectation. In order to formulate the result, we need to introduce two more arithmetic functions which may be considered as generalizations of σ'_p. For an integer $n \geq 1$ and a prime $p \equiv 5 \mod 8$ we define

$$\hat{\sigma}_p(n) = \sum_{0<d|n} \left(\frac{p}{d}\right) n/d$$

and

$$\tilde{\sigma}_p(n) = \sum_{0<d|n} \left(\frac{p}{d}\right) d.$$

Theorem 2. *Let p be 5 or 13. For any integer $n \geq 1$,*

$$A_p\delta_p(n) + 2\sum_{k=1}^{n-1} \delta_p(k)\delta_p(n-k) = B_p\hat{\sigma}_p(n) + C_p\tilde{\sigma}_p(n),$$

where

$$A_p = \begin{cases} 2(3+i)/5 & \text{if } p=5, \\ 2(1+i) & \text{if } p=13, \end{cases}$$

$$B_p = \begin{cases} 2+i & \text{if } p=5, \\ 2+3i & \text{if } p=13, \end{cases}$$

$$C_p = \begin{cases} -(4+3i)/5 & \text{if } p=5, \\ -i & \text{if } p=13. \end{cases}$$

4. Numerical evidence

Although the overall structure of our proofs of Theorems 1 and 2 is simple and clear, specific constants were not so easy to produce. Thus, when the overall structure of formulas was clear, we used computer calculations to find the constants and verify the identities claimed in the Theorems. The fact that an identity is true for the first several thousand values of n makes it very plausible that the identity is true for every n and encourages us to find a proof which is not based on the calculation alone.

In this section, we present gp-codes which verify our results numerically. Here, we try to follow the notation in this paper as closely as possible.

We first define the necessary characters, constants and analogues of σ_p and δ_p.

```
/*modularidentities.txt*/
\\This code checks the identity of the convolution involving conjugates of
   delta_p.

/*Defines characters sending the generator 2 to i.*/
chi_5(n)=if(n%5==2,I,if(n%5==4,-1,if(n%5==3,-I,if(n%5==1,1,0))));
{   chi_13(n)=if(n%13==1,1,if(n%13==2,I,if(n%13==3,1,
     if(n%13==4,-1,if(n%13==5,I,if(n%13==6,I,if(n%13==7,-I,if(n%13==8,-I,
     if(n%13==9,1,if(n%13==10,-1,if(n%13==11,-I,if(n%13==12,-1,0))))))))))));
}
/* Defines, delta_p, phi'_p, and sigma_p as in the paper*/
delta_5(n)=sumdiv(n,d,chi_5(d));
delta_13(n)=sumdiv(n,d,chi_13(d));

phi_5(n)=if(n%5==0,0,1);
phi_13(n)=if(n%13==0,0,1);

sigma_5(n)=sumdiv(n,d,phi_5(d)*d);
sigma_13(n)=sumdiv(n,d,phi_13(d)*d);

/*Defines constants for the identities involving convolution of conjugates*/
alpha(p)=if(p==5, 5/3, if(p==13, 1,0));
beta(p)=if(p==5, (3-I)/3, if(p==13, 1-I,0));


/*Defines sigma hat and sigma tilde as in the paper*/
```

```
hsigma_5(n)=sumdiv(n,d,kronecker(5,d)*n/d);
hsigma_13(n)=sumdiv(n,d,kronecker(13,d)*n/d);

tsigma_5(n)=sumdiv(n,d,kronecker(5,d)*d);
tsigma_13(n)=sumdiv(n,d,kronecker(13,d)*d);

/* Defines the constants for the identity involving convolution of delta_p*/
A(p)=if(p==5, 2*(3+I)/5,if(p==13,2*(1+I),0));
B(p)=if(p==5, 2+I,if(p==13,2+3*I,0));
C(p)=if(p==5,-(4+3*I)/5,if(p==13,-I,0));
```

To verify the first several thousand identities, we write each equation in Theorems 1 and 2 as a sum equal to 0. We then run a loop that will display the sum only if it is not zero, or it will display every 100th digit to signify the current step in the loop.

```
/* Defines Identities as sum to be equal to zero.*/
{    S_5(n)=real(beta(5)*delta_5(n))+alpha(5)*sum(k=1,n-1,
    delta_5(k)*conj(delta_5(n-k)))-sigma_5(n);
}
{    S_13(n)=real(beta(13)*delta_13(n))+alpha(13)*sum(k=1,n-1,
     delta_13(k)*conj(delta_13(n-k)))-sigma_13(n);
}

{    print("The following is a check for the convolution of identities involving
     delta_p and its conjugate");
}
/*Runs for loop that will only print the sum if it is non-zero or
will print every 100th term to keep track of the process*/

print("For p=5,");
for(n=1,5000, Q=S_5(n); if(Q!=0, print(Q),if(n%100==0,print(n),)));

print("For p=13,");
for(n=1,5000, Q=S_13(n); if(Q!=0, print(Q),if(n%100==0,print(n),)));


/* Defines Identities as sum to be equal to zero.*/
{    R_5(n)=A(5)*delta_5(n)+2*sum(k=1,n-1,delta_5(k)*delta_5(n-k))
     -B(5)*hsigma_5(n)-C(5)*tsigma_5(n);
}
{    R_13(n)=A(13)*delta_13(n)+2*sum(k=1,n-1,delta_13(k)*delta_13(n-k))
     -B(13)*hsigma_13(n)-C(13)*tsigma_13(n);
}
print("******************");
print("The following is a check for the convolution of identities involving
    delta_p");

/*Runs for loop that will only print the sum if it is non-zero or
```

```
will print every 100th term to keep track of the process*/

print("For p=5,");
for(n=1,5000, Q=R_5(n); if(Q!=0, print(Q),if(n%100==0,print(n),)));

print("For p=13,");
for(n=1,5000, Q=R_13(n); if(Q!=0, print(Q),if(n%100==0,print(n),)));
```

5. Generating functions reformulation

Both Theorem 1 and Theorem 2 claim an infinite series of identities enumerated by $n \geq 1$, but we will prove them as single identities for generating functions. We now give equivalent statements in terms of generating functions.

Define the formal power series in the variable q:

$$E_{1,p} = \sum_{n=0}^{\infty} \delta_p(n) q^n$$

with

$$\delta_p(0) = \begin{cases} (3+i)/10 & \text{if } p = 5, \\ (1+i)/2 & \text{if } p = 13, \end{cases}$$

$$E'_{2,p} = \sum_{n=0}^{\infty} \sigma'_p(n) q^n,$$

where

$$\sigma'_p(0) = \frac{p-1}{24},$$

$$\hat{E}_{2,p} = \sum_{n=1}^{\infty} \hat{\sigma}_p(n) q^n,$$

and

$$\tilde{E}_{2,p} = \sum_{n=0}^{\infty} \tilde{\sigma}_p(n) q^n,$$

where

$$\tilde{\sigma}_p(0) = \begin{cases} -1/5 & \text{if } p = 5, \\ -1 & \text{if } p = 13. \end{cases}$$

An easy calculation shows that, in terms of these generating functions, Theorem 1 is equivalent to the following statement.

Theorem A. *Let p be 5 or 13. Then*

$$E_{1,p}\overline{E_{1,p}} = t_p E'_{2,p},$$

where the bar denotes coefficient-wise complex conjugation of the power series, and

$$t_p = \begin{cases} 3/5 & \text{if } p = 5, \\ 1 & \text{if } p = 13. \end{cases}$$

Another calculation shows that Theorem 2 is equivalent to the following statement.

Theorem B. *Let p be 5 or 13. Then*

$$E_{1,p}^2 = u_p \hat{E}_{2,p} + v_p \tilde{E}_{2,p},$$

where

$$u_p = \begin{cases} (i+2)/2 & \text{if } p = 5, \\ (3i+2)/2 & \text{if } p = 13. \end{cases}$$

and

$$v_p = \begin{cases} -(3i+4)/10 & \text{if } p = 5, \\ -i/2 & \text{if } p = 13, \end{cases}$$

We will prove Theorems A and B as identities between modular forms. However, before we can do this we will need a collection of facts on modular forms which we provide in the next section.

6. Background on modular forms

In this section, we collect certain definitions and statements from the theory of modular forms. Some facts, although true in higher generality are stated here only in the special cases which are needed for our proof of Theorems A and B. We include references to the literature for both the proofs and more general statements.

Let N be a positive integer. The group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z} \text{ with } ad - bc = 1 \text{ and } c \equiv 0 \mod N \right\}$$

acts on the complex upper half-plane

$$\mathfrak{H} = \{ z \in \mathbb{C} \mid \Im(z) > 0 \}$$

with linear-fractional transformations

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

When $N = 1$, then the congruence condition becomes insignificant (as all integers are 0 modulo 1) and we have that

$$\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z}).$$

Now, let f be a holomorphic function on the complex upper half-plane.

$$f \;:\; \mathfrak{H} \to \mathbb{C}.$$

Let ψ be a Dirichlet character modulo N. Then f is called a *modular form* on $\Gamma_0(N)$ (*of level* N) of weight k with character ψ if it satisfies the functional equation

$$f\left(\frac{az+b}{cz+d}\right) = \psi(d)(cz+d)^k f(z),$$

and f is "holomorphic at the cusps". The latter condition is a little more difficult to explain, but we will address the issue shortly. Clearly, the shift by 1 matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$$

for any $N \geq 1$. This matrix taken with the functional equation implies that a modular form must be a periodic function. It is a basic fact from Fourier analysis that such function has a Fourier expansion

$$f(z) = \sum_{n=n_0}^{\infty} a(n) \exp(2\pi i n z).$$

In the case when $N = 1$, the "holomorphic at the cusps" condition simply means that $n_0 \geq 0$ (i.e. no negative exponents are involved). When $N > 1$, we also require that for every matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ (not only for those in $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$) we have an expansion

$$(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = \sum_{n=m_0}^{\infty} a(n) \exp(2\pi i n z/M),$$

with some positive integer $M \geq 1$ and again with $m_0 \geq 0$. Both M and m_0 may depend on the specific matrix.

Notation We denote by $M_k(N, \psi)$ the set of all modular forms of weight k, level N with character χ. It is immediate from the definition above that the set $M_k(N, \psi)$ is actually a vector space.

Example. Eisenstein series. (cf. [9, Section 2.1])

For an even integer $k > 2$ consider the function

$$G_k(z) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k}.$$

Proposition 4. *The function $G_k(z)$ satisfies the transformation law requirement of a modular form of level one and weight k.*

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. A simple calculation gives us

$$G_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \cdot \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{((am+cn)z + (bm+nd))^k}$$

Taking $m' = am + cn$ and $n' = bm + nd$ we note that as m and n run through each possible pair in $\mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\}$, so does m' and n'. Thus,

$$G_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \cdot \frac{1}{2} \sum_{\substack{m',n' \in \mathbb{Z} \\ (m',n') \neq (0,0)}} \frac{1}{(m'z+n')^k} = (cz+d)^k G_k(z).$$

Thus $G_k(z)$ satisfies the transformation law as we wanted. $\square$

In order to conclude that $G_k(z)$ is a modular form, according to the definition, we still have to get some information about its Fourier expansion.

From now on, we adopt a standard notation

$$q = \exp(2\pi i z)$$

which allows us to write Fourier expansions as power series in q. The following Proposition from the textbook ([9, Proposition 5, Section 2.2] does that, furthemore, it provides the Fourier expansion of $G_k(z)$ quite explicitly.

Proposition 5.

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

where B_k is the k-th Bernoulli number, and

$$\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}.$$

The proof of this Proposition is given in the textbook [9][pp.16].

The construction of Eisenstein series $G_k(z)$ may be generalized to the spaces $M_k(\Gamma_0(N), \psi)$. We will need the Fourier expansion of these series. Although the pattern persists, the proofs become much more difficult due to some subtle convergence questions (cf. [9, Section 2.3] for the case when $k = 2$). Thus we simply collect below several special cases of statements proved in the literature.

The Eisenstein series of weight one that we need can be found in [5, Chapter XV Theorem 1.1]. We quote the statement here.

Proposition 6. *Let ψ be a Dirichlet character modulo a prime p such that $\psi(-1) = -1$. The series*

$$G_{1,\psi} = -\frac{B_{1,\psi}}{2} + \sum_{n=1}^{\infty} \left(\sum_{0<d|n} \psi(d) \right) q^n$$

is the Fourier expansion of a modular form $G_{1,\psi}(z) \in M_1(p, \psi)$.

In particular, if $\psi = \chi_p$ it is easy to see that

$$G_{1,\chi_p} = E_{1,p} \in M_1(p, \chi_p) \quad \text{and} \quad G_{1,\overline{\chi_p}} = \overline{E_{1,p}} \in M_1(p, \overline{\chi_p}) \tag{4}$$

Eisenstein series of weight two that we need can be found in various sources. Specifically, we quote [5, Chapter XV Theorem 3.1].

Proposition 7. *Let ψ be a non-principal Dirichlet character such that $\psi(-1) = 1$. The series*

$$G_{2,\psi} = -\frac{1}{4} B_{2,\psi} + \sum_{n=1}^{\infty} \left(\sum_{0<d|n} \psi(d) d \right) q^n$$

is the Fourier expansion of a modular form $G_{2,\psi}(z) \in M_2(p, \psi)$.

In particular, if $p \equiv 1 \mod 4$ and $\psi(n) = \left(\frac{p}{n}\right)$ is the Kronecker symbol, it is easy to see that

$$G_{2,\psi} = \tilde{E}_{2,p} \in M_2\left(p, \left(\frac{p}{n}\right)\right) \tag{5}$$

To find our other Eisenstein series of weight two, we also quote [6, Theorem 7.2.12].

Proposition 8. *Let ψ be a non-principal Dirichlet character such that $\psi(-1) = 1$. The series,*

$$G_{2,\psi} = \sum_{n=1}^{\infty} \left(\sum_{0<d|n} \psi(d) \frac{n}{d} \right) q^n$$

is the Fourier expansion of a modular form $G_{2,\psi}(z) \in M_2(p, \psi)$.

In particular, if $p \equiv 1 \mod 4$ and $\psi(n) = \left(\frac{p}{n}\right)$ is the Kronecker symbol, we have that

$$G_{2,\psi} = \hat{E}_{2,p} \in M_2\left(p, \left(\frac{p}{n}\right)\right) \tag{6}$$

Finally, to find the last Eisenstein series of weight two that we need, we quote [6, Lemma 7.2.19]

Proposition 9. *Let φ_p be the trivial character modulo a prime p.*

The series

$$G_{2,\varphi_p} = \frac{p-1}{24} + \sum_{n=1}^{\infty} \left(\sum_{0<d|n} \varphi_p(d) d \right) q^n$$

is the Fourier expansion of a modular form $G_{2,\varphi_p} \in M_2(p, \varphi_p)$.

Clearly, we have that

$$G_{2,\varphi_p} = E'_{2,p}. \tag{7}$$

A fundamental fact from the theory of modular forms is the following

Theorem 3. *The vector space $M_k(N, \chi)$ is finite-dimensional.*

The proof of this fact is beyond the scope of this paper. It appears to be an application of the famous Riemann-Roch theorem. Moreover, this theorem, in many cases, gives us a way to calculate the dimension of a specific space $M_k(N, \psi)$. In the simplest case when $N = 1$, a proof of this theorem which makes use of nothing but classical complex analysis is given in e.g. in the textbook [9, Section 1.3]. Even this proof is quite involved. Very explicit formulas (more precisely, computational algorithms) for these dimensions were written down, in particular, by H. Cohen and J. Oesterlé in [1]. We used these formulas to calculate the dimensions in the cases of interest for us, and collect them in the following Proposition.

Proposition 10. *Let p be 5 or 13. Then*

$$\dim M_2(p, \varphi_p) = 1$$

and

$$\dim M_2\left(p, \left(\frac{p}{\cdot}\right)\right) = 2$$

We will need the following proposition which follows directly from the definition above.

Proposition 11. *If*

$$f \in M_k(N, \psi_1) \quad \text{and } g \in M_l(N, \psi_2)$$

then their product

$$fg \in M_{k+l}(N, \psi_1\psi_2).$$

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Then by hypothesis we have that,

$$f\left(\frac{az+b}{cz+d}\right) = \psi_1(d)(cz+d)^k f(z) \text{ and } g\left(\frac{az+b}{cz+d}\right) = \psi_2(d)(cz+d)^l g(z).$$

Since ψ_1 and ψ_2 are Dirichlet characters, their product, $\psi_1\psi_2$ is a Dirichlet character also. Thus,

$$\begin{aligned} fg\left(\frac{az+b}{cz+d}\right) &= f\left(\frac{az+b}{cz+d}\right) g\left(\frac{az+b}{cz+d}\right) \\ &= \psi_1(d)(cz+d)^k f(z)\psi_2(d)(cz+d)^l g(z) \\ &= \psi_1\psi_2(d)(cz+d)^{k+l} fg(z). \end{aligned}$$

Which proves that fg satisfies the transformation law requirement of modular forms. Moreover, if $N = 1$ then f and g can be written as

$$f(z) = \sum_{n=n_0}^{\infty} a(n)\exp(2\pi inz) \quad \text{and} \quad g(z) = \sum_{m=m_0}^{\infty} b(m)\exp(2\pi imz),$$

where $m_0, n_0 \geq 0$.

Without loss of generality suppose that $m_0 \leq n_0$, then

$$\begin{aligned} fg(z) &= \left(\sum_{n=n_0}^{\infty} a(n)\exp(2\pi inz)\right)\left(\sum_{m=m_0}^{\infty} b(m)\exp(2\pi imz)\right) \\ &= \sum_{n=m_0+n_0}^{\infty} c(n)\exp 2\pi inz, \end{aligned}$$

where $c(n) = \sum_{k=n_0}^{n-m_0} a(k)b(n-k)$.

If $N > 1$ then for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have the following expansions,

$$(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = a(n)\sum_{n=n_0}^{\infty} \exp(2\pi inz/M_1)$$

and

$$(cz+d)^{-l} g\left(\frac{az+b}{cz+d}\right) = \sum_{m=m_0}^{\infty} b(n)\exp(2\pi imz/M_2),$$

where $m_0, n_0 \geq 0$ and $M_1, M_2 \geq 1$. We may assume that $m_0 \leq n_0$.

Then,

$$(cz+d)^{-(k+l)}fg\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-k}f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-l}g\left(\frac{az+b}{cz+d}\right)$$
$$= \left(\sum_{n=n_0}^{\infty} a(n)\exp(2\pi inz/M_1)\right)\left(\sum_{m=m_0}^{\infty} b(n)\exp(2\pi inz/M_2)\right)$$
$$= \sum_{n=n_0M_2+m_0M_1} c(n)\exp(2\pi inz/(M_1M_2)),$$

where $c(n) = \sum_{k=n_0M_2}^{n-m_0M_1} a(k)b(n-k)$ (assuming that $m_0M_1 \leq n_0M_2$).

We see that the product is holomorphic at the cusps which proves that $fg \in M_{k+l}(N, \psi_1\psi_2)$. $\square$

7. Proof of the principal results

To prove our final results we consider from now on, $p = 5$ or 13, and take $G_{1,\chi_p} \in M_1(p, \chi_p)$ and $G_{1,\overline{\chi}_p}$ to be the modular forms as in Theorem 7.

Theorem A

Proof. By Proposition 11 we have that

$$G_{1,\chi_p}G_{1,\overline{\chi_p}} \in M_2(p, \chi_p\overline{\chi}_p) = M_2(p, \varphi_p).$$

.

Furthermore, $G_{2,\varphi_p} \in M_2(p, \varphi_p)$ by Proposition 9.

By Proposition 10, we know that $\dim M_2(p, \varphi_p) = 1$. Since $M_2(p, \varphi_p)$ is a vector space, we can conclude that G_{2,φ_p} and $G_{1,\chi_p}G_{1,\overline{\chi_p}}$ are linearly dependent and hence

$$G_{1,\chi_p}G_{1,\overline{\chi_p}} = t_pG_{2,\phi_p},$$

where t_p is a constant.

To calculate t_p it suffices to look at the coefficients of like powers of q:

$$\sum_{k=0}^{n} \delta_p(k)\overline{\delta_p(n-k)} = t_p\sigma_p'(n).$$

In particular,

$$\delta_p(0)\overline{\delta_p(0)} = t_p\sigma_p'(0)$$
$$t_p = \frac{|\delta_p(0)|^2}{\sigma_p'(0)}.$$

Thus,

$$t_p = \begin{cases} \frac{\left|\frac{i+3}{10}\right|^2}{\frac{1}{6}} = \frac{3}{5} & \text{if } p = 5, \\ \frac{\left|\frac{i+1}{2}\right|^2}{\frac{1}{2}} = 1 & \text{if } p = 13. \end{cases}$$

$\square$

Theorem B

Proof. Similarly by Proposition 11 we get

$$G_{1,\chi_p}^2 \in M_2(p,\chi_p^2) = M_2\left(p, \left(\frac{p}{n}\right)\right).$$

By Propositions 7 and 8 we have that $\tilde{E}_{2,p}, \hat{E}_{2,p} \in M_2\left(p, \left(\frac{p}{n}\right)\right)$.

Since $\dim M_2(p, \left(\frac{p}{n}\right)) = 2$ (Proposition 10) and we have three modular forms, we must have that

$$G_{1,\chi_p}^2 = u_p \hat{E}_{2,p} + v_p \tilde{E}_{2,p},$$

where u_p and v_p are constants.

To calculate u_p and v_p we again look at the coefficients of like powers of q:

$$\sum_{k=0}^{n} \delta_p(k)\delta_p(n-k) = u_p \hat{\sigma}_p(n) + v_p \tilde{\sigma}_p(n).$$

Taking $\hat{\sigma}_p(0) = 0$ (Proposition 8) we get

$$\begin{aligned} \delta_p(0)\delta_p(0) &= v_p \tilde{\sigma}_p(0) \\ v_p &= \frac{[\delta_p(0)]^2}{\tilde{\sigma}_p(0)}. \end{aligned}$$

Hence,

$$v_p = \begin{cases} \frac{\left(\frac{i+3}{10}\right)^2}{-\frac{1}{5}} = -\frac{3i+4}{10} & \text{if } p = 5, \\ \frac{\left(\frac{i+1}{2}\right)^2}{-1} = -\frac{i}{2} & \text{if } p = 13. \end{cases}$$

Taking $n = 1$ and taking v_p as above,

$$\sum_{k=0}^{n} \delta_p(k)\delta_p(n-k) = u_p \hat{\sigma}_p(n) + v_p \tilde{\sigma}_p(n),$$

gives us

$$\begin{aligned} 2\delta_p(0)\delta_p(1) &= u_p \hat{\sigma}_p(1) + v_p \tilde{\sigma}_p(1) \\ u_p &= \frac{2\delta_p(0)\delta_p(1) - v_p \tilde{\sigma}_p(1)}{\hat{\sigma}_p(1)}. \end{aligned}$$

Since $\delta_p(1) = \tilde{\sigma}_p(1) = \hat{\sigma}_p(1) = 1$ we get,

$$\begin{aligned} u_p &= 2\delta_p(0) - v_p \\ &= \begin{cases} 2\left(\frac{i+3}{10}\right) - \left(-\frac{3i+4}{10}\right) = \frac{i+2}{2} & \text{if } p = 5 \\ 2\left(\frac{i+1}{2}\right) - \left(-\frac{i}{2}\right) = \frac{3i+2}{2} & \text{if } p = 13. \end{cases} \end{aligned}$$

$\square$

Rewriting

$$G_{1,\chi_p} G_{1,\overline{\chi_p}} = t_p G_{2,\phi_p}$$

and

$$G_{1,\chi_p}^2 = u_p \hat{E}_{2,p} + v_p \tilde{E}_{2,p}$$

in terms of the first formulations of Theorem 1 and Theorem 2 allows us to verify theses identities using the codes in Section 4.

8. Caveats

For a prime $p > 2$ we know that either $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$. In Farkas and Guerzhoy and Raji's identities, all primes under consider consideration are $3 \mod 4$. The initial goal of this paper was to find identities which are close to Farka's original identity by considering all primes $p \equiv 1 \mod 4$; however a problem arose when we considered the quartic character which takes a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ to i. For example, if $p = 17$ the Kronecker Symbol is a Dirichlet character modulo p and it has two square root characters (Proposition 3) call them χ_{17} and $\overline{\chi}_{17}$. A simple calculation shows that χ_{17} and $\overline{\chi}_{17}$ are both even characters. Now, our formulas for constructing the required Eisenstein series force us to consider only odd square root characters. That is, if $\chi_p^2(n) = \left(\frac{p}{n}\right)$ we also need $\chi_p(-1) = -1$ (see Proposition 6). In general, we found that χ_p is an odd character only if $p \equiv 5 \mod 8$. Thus in our attempts to consider all primes (not $3 \mod 4$), we are still forced to restrict ourselves to $p \equiv 5 \mod 8$.

Furthermore, these are by no means the only arithmetic identities possible. If we eliminate our restriction to quartic characters and instead consider arbitrary odd Dirichlet characters modulo p it is possible to construct several more identities. Though, in this case these identities may not be as elegant as those which have already been found.

References

[1] Cohen, H.; Oesterlé, J. Dimensions des espaces de formes modulaires. Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 70-73. Lecture Notes in Math., Vol. 627, Springer, Berlin, 1977

[2] P. Guerzhoy and W. Raji, A modular look at Farkas' identities, Ramanujan J. 19 (2009), 19-27.

[3] Farkas, Hershel M., On an arithmetical function. II. Complex analysis and dynamical systems II, 121-130, Contemp. Math., 382, Amer. Math. Soc., Providence, RI, 2005

[4] Koblitz, Neal, Introduction to elliptic curves and modular forms, pp. 124-125. Springer-Verlag, New York, 1993

[5] Lang, Serge, Introduction to modular forms. With appendixes by D. Zagier and Walter Feit. Corrected reprint of the 1976 original. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 222. Springer-Verlag, Berlin, 1995.

[6] Miyake, Toshitsune, Modular forms. Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989

[7] Serre, Jean-Pierre, Formes modulaires et fonctions zêta p-adiques. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 191?268. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[8] Williams, K., Some arithmetic convolution identities, Ramanujan J., 2016, 1-17.

[9] Zagier, Don, Elliptic modular forms and their applications. The 1-2-3 of modular forms, 1-103, Universitext, Springer, Berlin, 2008