INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A18

CHARACTER SUMS AND RAMSEY PROPERTIES OF GENERALIZED PALEY GRAPHS

Nicholas Wage
Appleton East High School, Appleton, WI 54915, USA
wageee@gmail.com

Received: 8/23/05, Revised: 5/16/06, Accepted: 5/26/06, Published: 6/1/06

Abstract

In a classic paper, Evans, Pulham, and Sheehan computed the number of complete graphs of size 4 for a special class of graphs called Paley Graphs. Here we consider analogous questions for generalized Paley-type graphs.

1. Introduction

The Ramsey number $R(m)$ is the smallest positive integer such that any graph G with $R(m)$ or more vertices contains a complete subgraph of size m or its complement G^c contains a complete subgraph of size m. The only values of m for which $R(m)$ is known are $m \leq 4$. We consider a natural extension of computing and estimating $R(m)$. For a graph G, let $k_m(G)$ denote the number of complete graphs of size m contained in G. Let

$$T_m(n) := \min(k_m(G) + k_m(G^c)) \tag{1}$$

as G ranges over all graphs with n vertices. Note that $R(m)$ is the smallest n for which $T_m(n) > 0$. In [Erd62], Erdős conjectured that

$$\lim_{n\to\infty} \frac{T_m(n)}{n^m} = \frac{1}{2^{\binom{m}{2}-1} m!}. \tag{2}$$

However, this is not quite correct. In [Tho97], Thomason showed that for $m = 4$, this limit is no more than $1/(33 \cdot 4!)$, rather than $1/(32 \cdot 4!)$ as the conjecture predicts.

For a prime $p \equiv 1 \pmod 4$, let $G(p)$ denote the Paley graph with p vertices, indexed 0 through $p-1$. A Paley graph contains an edge $x \leftrightarrow y$ if and only if $\phi(x-y) = 1$, where $\phi(\cdot)$ denotes the Legendre symbol $\left(\frac{\cdot}{p}\right)$. This notation assumes that the prime p will be clear

from context. For example, the Paley graph $G(5)$ is a pentagon. The Legendre symbol is multiplicative and $\phi(-1) = 1$ if $p \equiv 1 \pmod 4$. Therefore, $\phi(y-x) = \phi(x-y)$. This equation implies that our definition is symmetric in x and y, so the edges are well defined.

For primes $p \equiv 3 \pmod 4$, $\phi(-1) = -1$, so $\phi(x-y) = -\phi(y-x)$. In this case we define a generalized directed Paley graph. Note that since $\phi(-1) = -1$ for every x and y, there is exactly one directed edge, creating a type of graph called a tournament.

Paley graphs have many interesting properties. They are both self-complementary and self-similar. Also, for the function $k_m(G) + k_m(G^c)$ on graphs with p vertices, Paley graphs are minimal in certain ways. For example, the Ramsey number $R(4) = 18$; the Paley graph $G(17)$ is the only graph (up to isomorphism) with 17 vertices such that $k_4(G) + k_4(G^c) = 0$.

This inspired Evans, Pulham, and Sheehan [EPS81] to compute the exact value of $k_4(G(p)) + k_4(G(p)^c)$ using character sums. For $m > 4$, the character sums are difficult to determine explicitly. We prove an asymptotic result for all m.

Theorem 1. For primes $p \equiv 1 \pmod 4$ and positive integers m

$$\lim_{p\to\infty} \frac{k_m\Big(G(p)\Big)}{p^m} = \frac{1}{2^{\binom{m}{2}} m!}.$$

Doubling this value to account for the complete graphs in its isomorphic complement, we see that the conjecture of Erdős, while false for general graphs, is true for the Paley graphs. Moreover, the conjectured bound is exactly achieved by these graphs.

For all primes p and integers $|t| > 1$ we define two other types of generalized Paley graphs, $G_t(p)$ and $G'_t(p)$. The graph $G_t(p)$ has an edge $x \leftrightarrow y$ if and only if both $\phi(x-ty) = 1$ and $\phi(y-tx) = 1$. The graph $G'_t(p)$ has an edge $x \leftrightarrow y$ if and only if at least one of these statements is true, that is $\phi(x-ty) = 1$ or $\phi(y-tx) = 1$. Note that $G_t(p)$ is a subgraph of $G'_t(p)$.

We now define two related generalized Paley graphs.

Definition 1. For a prime p and integer t, let $G_t(p)$ denote the graph with p vertices, indexed 0 through $p-1$, which contains an edge $x \leftrightarrow y$ if and only if $\phi(x-ty) = 1$ and $\phi(y-tx) = 1$. Similarly, let $G'_t(p)$ denote the graph with p vertices, indexed 0 through $p-1$, which contains an edge $x \leftrightarrow y$ if either $\phi(x-ty) = 1$ or $\phi(y-tx) = 1$, and contains no edge $x \leftrightarrow y$ if neither of these statements hold true.

We prove a similar result for these generalized graphs.

Theorem 2. Let m be a positive integer and t be an integer such that $t \not\equiv -1, 0, 1 \pmod p$. Then, for primes p, and we have

$$\lim_{p\to\infty} \frac{k_m\Big(G_t(p)\Big) + k_m\Big(G_t(p)^c\Big)}{p^m} = \frac{1}{m!}\left(\left(\frac{1}{4}\right)^{\binom{m}{2}} + \left(\frac{3}{4}\right)^{\binom{m}{2}}\right).$$

Similarly,

$$\lim_{p\to\infty} \frac{k_m\Big(G_t'(p)\Big) + k_m\Big(G_t'(p)^c\Big)}{p^m} = \frac{1}{m!}\left(\left(\frac{1}{4}\right)^{\binom{m}{2}} + \left(\frac{3}{4}\right)^{\binom{m}{2}}\right).$$

Remark. After this work was completed, it was brought to the author's attention that a paper of Graham, Chung, and Wilson, [CGW88], implies these limits because Paley graphs are examples of quasi-random graphs. However, we stress that the proofs in this paper are direct, and lead to stronger error terms in estimates. In other words, a careful analysis of these proofs leads to strong bounds for the errors between the limiting values and the actual values.

A key result in the work of Evans, Pulham and Sheehan is a formula that exactly computes the number of complete graphs of size 4 in a Paley graph, namely, they obtain

$$k_4\Big(G(p)\Big) = \frac{p-1}{1536}\left(p\left((p-9)^2 - 4x^2\right)\right) \tag{3}$$

where x is an even integer such that $p = x^2 + y^2$. It is known that for $p \equiv 1 \pmod 4$, that x not only exists, but is unique (up to sign). Their proof essentially follows from an evaluation of the hypergeometric sum

$${}_3F_2(t) = \frac{\phi(-1)}{p^2}\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \phi(x)\phi(y)\phi(1-x)\phi(1-y)\phi(x-ty) \tag{4}$$

when $t = 1$. One should note that while it can be shown that this is equivalent to the definition of ${}_3F_2(t)$, it is not a priori the definition. Similarly, we will require the sum

$${}_2F_1(t) = \frac{\phi(-1)}{p}\sum_{x\in\mathbb{Z}/p\mathbb{Z}} \phi(x)\phi(1-x)\phi(1-tx). \tag{5}$$

In this paper we compute a graph theoretic result similar to that of Evans, Pulham, and Sheehan which would normally be intractable without the help of the special t evaluations of these character sums.

Theorem 3. Let p be a prime, and let t be a non-zero element of $\mathbb{Z}/p\mathbb{Z}$ whose multiplicative order is greater than 3. Let $H_t(p)$ represent the directed graph where $x \to y$ is an edge if and only if $\phi(x) = \phi(x-ty) = 1$, and let $C_t(p)$ denote the number of 3-cycles in $H_t(p)$ $(x \to y \to z \to x)$. Then

$$\begin{aligned} C_t(p) \;=\; & \frac{p-1}{192}\Big[90 - 3p\phi(t) + 12\phi(t+t^2) + p^2 - 14p + 48\phi(-t) + 27\phi(t) + 62\phi(1-t) \\ & + 6\phi(1-t^3) + 12\phi(t-t^3) + 12\phi(1-t^2) + 12\phi(-1) + 12\phi(1+t) + 24\phi(t^2-t) \\ & + 6\phi(t-t^4) + 12\phi(t-t^2) + 3\phi(t^4-t)p - 6p\phi(1-t) - 3\phi(-t)p + p^2{}_3F_2(t^3) \\ & - 6p(1+\phi(1-t)){}_2F_1(t^2) - 3p(1+\phi(t)){}_2F_1(t^3)\Big]. \end{aligned}$$

Although this formula is difficult to grasp at first glance, we note that it simplifies dramatically for several special t. For example, we obtain formulas much like (3) in the following cases:

Corollary 1. If $t = -2$, and p is a prime congruent to 5 or 7 $\pmod{24}$, then

$$C_t(p) = \begin{cases} \frac{p-1}{192}\,(p^2 - 6p + 4x^2 + 1) & \text{if } p \equiv 5 \pmod{24}, x^2 + y^2 = p, \text{ and } x \text{ odd}, \\ \frac{p-1}{192}\,(p^2 - 6p + 25) & \text{if } p \equiv 7 \pmod{24}. \end{cases}$$

Corollary 2. If $t = -\frac{1}{2}$, and p is a prime congruent to 7 or 13 $\pmod{24}$, then

$$C_t(p) = \begin{cases} \frac{p-1}{192}(p^2 - 6p + 25) & \text{if } p \equiv 7 \pmod{24}, \\ \frac{p-1}{192}(p^2 + 2p - 4x^2 + 1) & \text{if } p \equiv 13 \pmod{24}, x^2 + y^2 = p, \text{ and } x \text{ odd}. \end{cases}$$

In Section 2 we state the tools that will be necessary in Section 3, where we will prove the main theorems.

2. Preliminaries

We will need the following facts for our proofs. The deepest result we require is due to Weil.

Weil's Theorem. ([BEW98], pg. 183) If p is a prime, and $f(x) \in \mathbb{Z}[x]$ is a polynomial with degree n which is not congruent modulo p to $cg^2(x)$ for any integer c and polynomial $g(x)$ with integer coefficients, then

$$\left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \phi\Big(f(x)\Big) \right| < (n-1)\sqrt{p}.$$

Remark. ¿From this point onward, we omit the summation indices with the understanding that all sums are over $\mathbb{Z}/p\mathbb{Z}$ unless indicated otherwise.

For small n, explicit evaluations of these sums are simple. Clearly, if $n = 0$,

$$\sum_x \phi(c) = \phi(c)p. \tag{6}$$

Note that as x runs over all the elements of $\mathbb{Z}/p\mathbb{Z}$, so does $ax + b$ if $a \not\equiv 0 \pmod{p}$. Using this fact, we can also compute the value for $n = 1$. Let q denote a non-zero, non-residue of

$\mathbb{Z}/p\mathbb{Z}$. Then

$$\begin{aligned}\sum_x \phi(ax+b) &= \sum_{y=ax+b} \phi(y) \\ &= \sum_{z=q^{-1}y} \phi(qz) \\ &= \phi(q)\sum_z \phi(z) \\ &= -\sum_y \phi(y) \\ &= -\sum_x \phi(ax+b),\end{aligned}$$

so

$$\sum_x \phi(ax+b) = 0. \tag{7}$$

Finally, we prove a formula for the case $n = 2$.

Proposition 1. For any prime p and polynomial $f(x) = ax^2 + bx + c$ with roots r and s is $\mathbb{Z}/p\mathbb{Z}$,

$$\sum_x \phi(ax^2+bx+c) = \begin{cases}(p-1)\phi(a) & \text{if } r \equiv s \pmod p \\ -\phi(a) & \text{if } r \not\equiv s \pmod p.\end{cases}$$

Proof.

$$\begin{aligned}\sum_x \phi(ax^2+bx+c) &= \sum_x \phi\Big(a(x-r)(x-s)\Big) \\ &= \phi(a)\sum_x \phi(x)\phi\Big(x-(s-r)\Big).\end{aligned}$$

Let $t = s-r$. Note that when $t \equiv 0 \pmod p$, it is clear that $\sum_x \phi(x)^2 = p-1$. When, $t \not\equiv 0 \pmod p$,

$$\sum_x \phi(x)\phi(x-t) = \sum_{tx} \phi(tx)\phi(t(x-1)) = \sum_x \phi(x)\phi(x-1),$$

so the summation is equivalent to the summation when $t \equiv 1 \pmod p$. Thus, this is equivalent for all $p-1$ non-zero values of t. Note that

$$\begin{aligned}\sum_t \sum_x \phi\Big(x(x-t)\Big) &= \sum_x \phi(x)\sum_t \phi(x-t) \\ &= \sum_x \phi(x)\sum_{u=x-t} \phi(u) \\ &= \sum_x \phi(x)\cdot 0 \\ &= 0.\end{aligned}$$

However, we can also show that

$$\begin{aligned}\sum_t \sum_x \phi\Big(x(x-t)\Big) &= \sum_x \phi(x)^2 + (p-1)\sum_x \phi(x)\phi(x-t) \\ &= (p-1)\left(1 + \sum_x \phi(x)\phi(x-t)\right).\end{aligned}$$

Equating these two expressions, we obtain

$$\phi(a)\sum_x \phi(x)\phi(x-t) = -\phi(a).$$

□

For $n \geq 3$ there does not appear to be a general evaluation. However, with additional machinery, certain evaluations are possible. A character χ is a multiplicative function that maps the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ to the complex roots of unity. Let $\bar{\chi}$ denote the conjugate character of χ, that is, $\bar{\chi}(x) = 1/\chi(x)$. By convention, we say that $\chi(0) = 0$. The Legendre symbol is a simple example of a character. Another simple character is ϵ, the trivial character, for which $\epsilon(x) = 1$ unless $x \equiv 0 \pmod{p}$.

A Jacobi sum, for characters χ and ψ is

$$J(\chi, \psi) := \sum_x \chi(x)\psi(1-x). \tag{8}$$

Additionally, we define the normalized Jacobi sum for characters A and B

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \bar{B}). \tag{9}$$

Then, we define

$${}_{n+1}F_n\left(\begin{array}{cc} A_0, & A_1, \ldots A_n \\ & B_1, \ldots B_n \end{array} \Big| t\right) := \frac{p}{p-1}\sum_\chi \binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi}\cdots\binom{A_n\chi}{B_n\chi}\chi(t), \tag{10}$$

where the sum is over all χ with modulus p. Additionally, we define

$${}_{n+1}F_n(t) := {}_{n+1}F_n\left(\begin{array}{cc} \phi, & \phi, \ldots \phi \\ & \epsilon, \ldots \epsilon \end{array} \Big| t\right). \tag{11}$$

Although these functions are expressed in terms of Jacobi sums, it is known that the definitions in the introduction, (5) and (4), are equivalent (see [Ono04]). These objects allow us to find a general formula in terms of ${}_2F_1$ when $n = 3$.

Proposition 2. For any prime p and third-degree polynomial with leading coefficient a and distinct roots $q, r, s \in \mathbb{Z}/p\mathbb{Z}$, we have

$$\sum_x \phi\Big(a(x-q)(x-r)(x-s)\Big) = \phi(-a)\phi(q-s)\,{}_2F_1\left(\frac{r-s}{q-s}\right)p.$$

Proof. The proof of this is straightforward:

$$\begin{aligned}\sum_x \phi\Big(a(x-q)(x-r)(x-s)\Big) &= \phi(a)\sum_x \phi\Big(x(q-s-x)(r-s-x)\Big)\\ &= \phi(a)\phi(q-s)\sum_{(q-s)x}\phi(x)\phi(1-x)\phi\left(1-\frac{r-s}{q-s}x\right)\\ &= \phi(-a)\phi(q-s){}_2F_1\left(\frac{r-s}{q-s}\right)p.\end{aligned}$$

□

3. Proof of the Theorems

Using Weil's Theorem from the previous section, we will prove Theorem 1.

Proof of Theorem 1. The following is a proof by induction. For $m = 1$, $k_1(G(p)) = p$, so the theorem holds. Assume the theorem holds for $m-1$. For each prime $p \equiv 1 \pmod 4$ we want to write $k_m(G(p))$ as a character sum. To count the number of complete m-subgraphs, we look at each possible set of m distinct points, and check to see if it is a complete subgraph. Since xy is an edge if and only if $\phi(x-y) = 1$, then assuming $x \neq y$ the equation $\frac{1+\phi(x-y)}{2}$ conveniently returns 1 if $x \leftrightarrow y$ is an edge, and 0 otherwise. Thus, if we take the product of this equation over all pairs selected from our m points, it will return 1 if we have a complete subgraph, and 0 otherwise. We need only sum this product over all possible sets of m distinct points to get $k_m(G(p))$. Therefore

$$k_m\Big(G(p)\Big) = \sum_{a_1<\cdots<a_m}\left(\prod_{0<i<j\le m}\frac{1+\phi(a_i-a_j)}{2}\right).$$

We will now manipulate this equation to make it easier to evaluate. First we can isolate the a_m terms into their own summation. Second, we can replace the condition that a_m is greater than a_{m-1} and simply require it to be distinct from each of the other a_i. Note that this will count each set of m vertices m times, once for each possible final term, so we must divide by m. Then, we can separate out the terms of the product not involving a_m, and pull out a 2^{1-m} term. The result of all these manipulations is

$$k_m\Big(G(p)\Big) =$$

$$\sum_{a_1<\ldots<a_{m-1}}\left[\left(\prod_{0<i<j<m}\frac{1+\phi(a_i-a_j)}{2}\right)\left(\frac{1}{2^{m-1}m}\sum_{a_m\neq a_i}\prod_{k=1}^{m-1}\Big(1+\phi(a_m-a_k)\Big)\right)\right].$$

Note that the beginning of this equation resembles $k_{m-1}(G(p))$. If we bound

$$\sum_{a_m \neq a_i} \prod_{k=1}^{m-1} \Big(1 + \phi(a_m - a_k)\Big)$$

in terms of p and m, then we can pull it outside of the summation. Specifically, if we show that

$$p - 2^m m(\sqrt{p}+2) \leq \sum_{a_m \neq a_i} \prod_{k=1}^{m-1} \Big(1 + \phi(a_m - a_k)\Big) \leq p + 2^m m(\sqrt{p}+1), \tag{12}$$

then

$$\frac{p - 2^m m(\sqrt{p}+2)}{2^{m-1}m} k_{m-1}\Big(G(p)\Big) \leq k_m\Big(G(p)\Big) \leq \frac{p + 2^m m(\sqrt{p}+1)}{2^{m-1}m} k_{m-1}\Big(G(p)\Big),$$

and by the inductive hypothesis we know that

$$\begin{aligned} \lim_{p\to\infty} \frac{\Big(p - 2^m m(\sqrt{p}+2)\Big)k_{m-1}\Big(G(p)\Big)}{p^m 2^{m-1} m} &= \lim_{p\to\infty} \frac{p - 2^m m(\sqrt{p}+2)}{2^{m-1}mp} \cdot \frac{k_{m-1}\Big(G(p)\Big)}{p^{m-1}} \\ &= \frac{1}{2^{\binom{m}{2}} m!}. \end{aligned}$$

The right hand bound evaluates to the same limit, and so

$$\lim_{p\to\infty} \frac{k_m\Big(G(p)\Big)}{p^m} = \frac{1}{2^{\binom{m}{2}} m!},$$

which proves our result.

All that remains is to prove the bound for (12). We start by multiplying out each product, getting 2^{m-1} terms. The first term is 1, which we sum over the $p - (m-1)$ possible values of a_m.

Now, consider an arbitrary term from the remaining 2^{m-1} terms. It is a product of Legendre symbols of the form $\phi(a_m - a_i)$. Since the Legendre symbol is multiplicative, we can form a single Legendre symbol, that is, write the term as $\phi(f(a_m))$ where f is a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$. We know the roots of f are among the different a_i values, that f contains at least one such root, and, since all the a_i are distinct, f has no repeated roots. This means that it is not congruent (mod p) to $cg(x)^2$ for any integer c and polynomial g with integer coefficients. Moreover, f has degree at most $m-1$ so by Weil's theorem, we have

$$-(m-2)\sqrt{p} \leq \sum_{a_m \in \mathbb{Z}/p\mathbb{Z}} \phi\Big(f(a_m)\Big) \leq (m-2)\sqrt{p}.$$

Note that this sum, however, includes $m-1$ terms which are not in the sum we wish to evaluate, namely $a_1, \ldots, a_{m-1}$. Each of these terms is between -1 and 1, so removing them changes the sum by at most $m-1$. Therefore,

$$-m(\sqrt{p}+1) \leq -(m-1)(\sqrt{p}+1) \leq \sum_{a_m \neq a_i} \phi\Big(f(a_m)\Big) \leq (m-1)(\sqrt{p}+1) \leq m(\sqrt{p}+1).$$

This bound holds for each of the $2^{m-1}-1$ terms involving Legendre symbols, so

$$p-m+1-2^{m-1}m(\sqrt{p}+1) \leq \sum_{a_m \neq a_i} \prod_{k=1}^{m-1} \Big(1+\phi(a_m-a_k)\Big) \leq p-m+1+2^{m-1}m(\sqrt{p}+1),$$

which implies (12).

□

The proof of Theorem 2 is similar to the proof of Theorem 1. This time we examine $k_m(G_t(p))$ as a character sum and use Weil's Theorem to estimate it.

Proof of Theorem 2. We first prove that

$$\lim_{p\to\infty} \frac{k_m\Big(G_t(p)\Big)}{p^m} = \frac{1}{m!}\left(\frac{1}{4}\right)^{\binom{m}{2}}. \tag{13}$$

First consider x and y such that $x \not\equiv y, ty, t^{-1}y, t^2y, t^{-2}y \pmod p$. There is an edge between x and y in $G_t(p)$ if and only if $\phi(x-ty)=\phi(y-tx)=1$. Thus,

$$\frac{(1+\phi(x-ty))}{2}\frac{(1+\phi(y-tx))}{2} = \begin{cases} 1 & \text{if } x \leftrightarrow y \text{ is an edge,} \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

As such, we define

$$h_m(p) := \sum_{\substack{a_1<\ldots<a_m \\ a_i \not\equiv ta_j, t^2a_j}} \left(\prod_{\substack{0<i,j\leq m \\ i\neq j}} \frac{1+\phi(a_i-ta_j)}{2} \right). \tag{15}$$

This counts the number of complete subgraphs in $G_t(p)$ that do not contain any edges where $x \equiv t^{-2}y, t^{-1}y, t^1y, t^2y \pmod p$. However, each $x \in \mathbb{Z}/p\mathbb{Z}$ has at most 4 such edges, so there are at most $2p$ of these edges total since each edge is counted twice. Each such edge is a member of $\binom{p-2}{m-2}$ subgraphs of size m, and so we are missing at most $2p\binom{p-2}{m-2}$ complete subgraphs of size m. Thus

$$h_m(p) \leq k_m\Big(G_t(p)\Big) \leq h_m(p) + 2p\binom{p-2}{m-2}.$$

We divide this equation by p^m and take the limit as p tends to infinity. The $2p\binom{p-2}{m-2}$ term has degree p^{m-1}, so it vanishes, making the left hand side and right hand side limits equal. Therefore

$$\lim_{p\to\infty} \frac{k_m\Big(G_t(p)\Big)}{p^m} = \lim_{p\to\infty} \frac{h_m(p)}{p^m},$$

and all that remains is to evaluate (15). In particular, we will show that

$$\lim_{p\to\infty} \frac{h_m(p)}{p^m} = \frac{1}{4^{\binom{m}{2}}m!}.$$

This will be proved by induction. If $m = 1$, it is clearly true. Otherwise, assume the claim is true for $m-1$. Performing the same manipulations as in the proof of Theorem 1, we get

$$h_m(p) = \sum_{\substack{a_1<\ldots<a_m \\ a_i\not\equiv ta_j, t^2a_j}} \left[\left(\prod_{\substack{0<i,j<m \\ i\neq j}} \frac{1+\phi(a_i-ta_j)}{2} \right) \times \left(\frac{1}{4^{m-1}m} \sum_{\substack{a_m\not\equiv t^e a_i \\ -2\le e\le 2}} \prod_{k=1}^{m-1} \Big(1+\phi(a_m-ta_k)\Big)\Big(1+\phi(a_k-ta_m)\Big) \right) \right].$$

So, if we show that

$$\left| \sum_{\substack{a_m\not\equiv t^e a_i \\ -2\le e\le 2}} \prod_{k=1}^{m-1} \Big(1+\phi(a_m-ta_k)\Big)\Big(1+\phi(a_k-ta_m)\Big) - p \right| \le 4^{m-1}(2m\sqrt{p}+5m), \tag{16}$$

then

$$\frac{p-4^{m-1}(2m\sqrt{p}+5m)}{4^{m-1}m} h_{m-1}(p) \le h_m(p) \le \frac{p+4^{m-1}(2m\sqrt{p}+5m)}{4^{m-1}m} h_{m-1}(p).$$

Applying the inductive hypothesis, we obtain

$$\begin{aligned} \lim_{p\to\infty} \frac{\Big(p-4^{m-1}(2m\sqrt{p}+5m)\Big)h_{m-1}(p)}{4^{m-1}mp^m} &= \lim_{p\to\infty} \frac{p-4^{m-1}(2m\sqrt{p}+5m)}{4^{m-1}mp} \cdot \frac{h_{m-1}(p)}{p^{m-1}} \\ &= \frac{1}{4^{\binom{m}{2}}m!}. \end{aligned}$$

The right hand side limit evaluates to the same value and thus

$$\lim_{p\to\infty} \frac{h_m(p)}{p^m} = \frac{1}{4^{\binom{m}{2}}m!}. \tag{17}$$

All that remains is to prove the bounds for (16). We multiply out the product, getting 4^{m-1} terms. The first term is simply 1. There are at most p choices for a_m, and at least $p-5m$, so summing it over all of them returns a value between $p-5m$ and p.

Now, consider an arbitrary term out of the remaining $4^{m-1}-1$ terms. It is a product of Legendre symbols of the form $\phi(a_m - ta_i)$ and $\phi(a_i - ta_m)$. Since the Legendre symbol is multiplicative, we can form a single Legendre symbol, that is, write the term as $\phi(f(a_m))$ where f is a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$. We know f has at least one root, and we know that each of the roots of f is either of the form ta_i or $t^{-1}a_i$ for some i. Also, since $t \neq \pm 1$, $ta_i \neq t^{-1}a_i$, so if f had a repeated root r, we could write $r = ta_i = t^{-1}a_j$. However, this implies that $a_j = t^2 a_i$ and our summation requires that we choose a_i and a_j such that this is false. Thus, f has no repeated roots, and this means that it is not congruent modulo p to $cg(x)^2$ for any integer c and polynomial g with integer coefficients. Moreover, f has degree at most $2m-2$, so by Weil's theorem we have

$$\left| \sum_{a_m} \phi\Big(f(a_m)\Big) \right| \leq (2m-3)\sqrt{p}.$$

Note that the above sum includes at most $5m$ terms that the summations in (16) excludes. Each of these terms is between -1 and 1, so removing them changes the sum by at most $5m$. Therefore,

$$\left| \sum_{\substack{a_m \not\equiv t^e a_i \\ -2 \leq e \leq 2}} \phi\Big(f(a_m)\Big) \right| \leq 2m\sqrt{p} + 5m.$$

This bound holds for each of the $4^{m-1}-1$ terms involving Legendre symbols, so (16) holds.

The other three calculations of $\lim_{p\to\infty} k_m(\cdot)/p^m$ are analogous. For x and y where $x \not\equiv t^{-2}y, t^{-1}y, y, ty, t^2 y$, we replace (14) with

$$\begin{aligned}
&\frac{3-\phi(x-ty)-\phi(y-tx)-\phi(x-ty)\phi(y-tx)}{4} && \text{for } G_t(p)^c;\\
&\frac{3+\phi(x-ty)+\phi(y-tx)-\phi(x-ty)\phi(y-tx)}{4} && \text{for } G_t'(p);\\
&\frac{(1-\phi(x-ty))}{2}\frac{(1-\phi(y-tx))}{2} && \text{for } G_t'(p)^c.
\end{aligned}$$

The calculations follow as above. □

We now prove Theorem 3, the result expressing $C_t(p)$ in terms of hypergeometric functions.

Proof of Theorem 3. The first step is to once again write our expression for $C_t(p)$ as a character sum. No cycle can contain 0 because $\phi(0) = 0$, and so 0 has no outgoing edges. So we

look at each set of three distinct, non-zero points x, y, and z, and check for a cycle. Also, we may assume that $x \not\equiv ty$, $y \not\equiv tz$, and $z \not\equiv tx$, because if one of these is true, there is no cycle. Note that any such group of x, y, z the expression

$$\Big(1+\phi\left(x\right)\Big)\Big(1+\phi\left(y\right)\Big)\Big(1+\phi\left(z\right)\Big)\Big(1+\phi\left(x-ty\right)\Big)\Big(1+\phi\left(y-tz\right)\Big)\Big(1+\phi\left(z-tx\right)\Big)$$

returns 2^6 if x, y, and z form a cycle, and 0 otherwise. If we sum this over each possible set, we count each cycle three times. Thus

$$3\cdot 2^6\cdot C_t(p)=\sum_{z\not\equiv 0}\sum_{\substack{y\not\equiv 0,z,\\ tz}}\sum_{\substack{x\not\equiv 0,y,\\ z,ty,t^{-1}z}}\Bigg(\Big(1+\phi\left(x\right)\Big)\Big(1+\phi\left(y\right)\Big)\Big(1+\phi\left(z\right)\Big)$$
$$\times\Big(1+\phi\left(x-ty\right)\Big)\Big(1+\phi\left(y-zt\right)\Big)\Big(1+\phi\left(z-tx\right)\Big)\Bigg).$$

Since $z \not\equiv 0$, xz runs over $\mathbb{Z}/p\mathbb{Z}$ as x does, and yz runs over $\mathbb{Z}/p\mathbb{Z}$ as y does, so we can replace x by xz and y by yz. We can pull the $(1+\phi(z))$ term to the very front of the summation. Note that $\phi(z)\neq 0$, and when $\phi(z)=-1$ and $1+\phi(z)=0$, the whole inner term is multiplied by 0, so its accuracy is irrelevant. Thus, assuming that $\phi(z)=1$ is always true within the inner summations does not change the value of the expression as a whole. Using this fact, we can entirely rid the inner summation of z and write

$$3\cdot 2^6\cdot C_t(p)=c\sum_{z\not\equiv 0}\Big(1+\phi\left(z\right)\Big)=(p-1)c.$$

where

$$c=\sum_{\substack{y\not\equiv 0,1,\\ t}}\sum_{\substack{x\not\equiv 0,1,\\ t^{-1},y,ty}}\Big(1+\phi\left(x\right)\Big)\Big(1+\phi\left(y\right)\Big)\Big(1+\phi\left(y-t\right)\Big)\Big(1+\phi\left(1-tx\right)\Big)\Big(1+\phi\left(x-ty\right)\Big).$$

The 5 values x does not take on are all distinct unless $y = t^{-1}$ or $y = t^{-2}$. Thus

$$\begin{aligned}
c &= \sum_{\substack{y\neq 0,1,\\ t,t^{-1},t^{-2}}} \sum_{x} \Big(1+\phi(x)\Big)\Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(1-tx)\Big)\Big(1+\phi(x-ty)\Big) \\
&\quad + \sum_{\substack{x\neq 0,1\\ t^{-1}}} \Big(1+\phi(x)\Big)\Big(1+\phi(t)\Big)\Big(1+\phi(1-tx)\Big)\Big(1+\phi\left(t-t^3\right)\Big)\Big(1+\phi(x-1)\Big) \\
&\quad + \sum_{\substack{x\neq 0,1\\ t^{-1},t^{-2}}} 2\Big(1+\phi(x)\Big)\Big(1+\phi(1-tx)\Big)\Big(1+\phi\left(1-t^3\right)\Big)\Big(1+\phi\left(x-t^{-1}\right)\Big) \\
&\quad - \sum_{\substack{y\neq 0,t^{-2}\\ t^{-1},1,t}} 2\Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(-ty)\Big) \\
&\quad - \sum_{\substack{y\neq 0,t^{-2}\\ t^{-1},1,t}} 2\Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(1-t)\Big)\Big(1+\phi(1-ty)\Big) \\
&\quad - \sum_{\substack{y\neq 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(t)\Big)\Big(1+\phi\left(t^{-1}-ty\right)\Big) \\
&\quad - \sum_{\substack{y\neq 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi(y)\Big)^2\Big(1+\phi(y-t)\Big)\Big(1+\phi(1-ty)\Big)\Big(1+\phi(y-ty)\Big) \\
&\quad - \sum_{\substack{y\neq 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(ty)\Big)\Big(1+\phi\left(1-t^2y\right)\Big) \\
&= S_0+S_1+S_2-S_3-S_4-S_5-S_6-S_7,
\end{aligned}$$

where S_i corresponds to the term in the ith row. Note that since the order of t is greater than three, $t \not\equiv 1, t^{-1}, t^{-2}$ so there is no double counting.

Now we wish to evaluate these 8 terms. Key to the simplification will be the following trick: if we have an expression of the form $(1+\phi(\alpha))\cdot(\dots)$, where we know $\alpha \not\equiv 0$, then we may assume throughout the $(\dots)$ that $\phi(\alpha) = 1$, because either this will be true, or the entire expression will be multiplied by 0 so it is irrelevant. We will also make use of equations (6) and (7), as well as propositions and outlined in the preliminaries. With these tools it is not difficult to reduce the expressions to closed forms in terms of ${}_2F_1$ and ${}_3F_2$ values. From this point on, all equations have been verified as accurate for small primes (less than 200) by direct computer calculations in order to prevent arithmetic errors during the manipulations.

For S_0, we pull the two terms involving just y out of the inner summation, and evaluate it. Then we switch the order of summation and solve the inner one. Thus

$$\begin{aligned}
S_0 &= \sum_{\substack{y\not\equiv 0,1,\\ t,t^{-1},t^{-2}}} \sum_x \Big(1+\phi(x)\Big)\Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(1-tx)\Big)\Big(1+\phi(x-ty)\Big)\\
&= \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(p-1-2\phi(-t)+\sum_x \phi(x)\phi(1-tx)\phi(x-ty)\Big)\\
&= \Big(p-1-2\phi(-t)\Big)\Big(p-8-2\phi(t)-2\phi(1-t)-2\phi(1-t^3)-\phi(-t)-\phi(t-t^3)-\phi(1-t^2)\Big)\\
&\quad + p^2{}_3F_2(t^3)+3+\phi(t^4-t)p+\phi(-t)+2\phi(-1)+2\phi(t^3-1)\\
&\quad - p\Big(1+\phi(t)\Big)\Big(1+\phi\left(1-t^2\right)\Big)_2F_1(t)-2p\Big(1+\phi(1-t)\Big)_2F_1(t^2)\\
&\quad - p\Big(1+\phi(t)\Big)_2F_1(t^3).
\end{aligned}$$

To evaluate S_1, we pull the terms independent of x to the front of the summation. Then since the expression is multiplied by $1+\phi(t)$, we may use the trick mentioned above to assume that $\phi(t)=1$ throughout the rest of the expression. Next, we take the summation over all x and subtract out the specific cases 0, 1, and t^{-1}. Then we multiply out the inside of the summation and evaluate it term by term. This shows that

$$\begin{aligned}
S_1 &= \Big(1+\phi(t)\Big)\Big(1+\phi\left(t-t^3\right)\Big)\sum_{\substack{x\not\equiv 0\\ t^{-1},1}} \Big(1+\phi(x)\Big)\Big(1+\phi(1-tx)\Big)\Big(1+\phi(x-1)\Big)\\
&= \Big(1+\phi(t)\Big)\Big(1+\phi\left(1-t^2\right)\Big)\Big(p+p_2F_1(t)-2\phi(-1)-4\phi(1-t)-2\phi(-t)-7\Big).
\end{aligned}$$

The value of S_2 is computed by noting that after pulling out a $\phi(-t)$ from the third term of the summand, it is similar to the second term and so we can pull a $(1+\phi(-t))$ to the front using the trick above, and evaluate it in a fashion similar to S_1. The resulting expression can be simplified further using the trick mentioned above. Hence

$$\begin{aligned}
S_2 &= 2\Big(1+\phi\left(1-t^3\right)\Big)\sum_{\substack{x\not\equiv 0,t^{-2}\\ t^{-1},1}} \Big(1+\phi(x)\Big)\Big(1+\phi(1-tx)\Big)\Big(1+\phi(-t)\phi(1-tx)\Big)\\
&= 2\Big(1+\phi\left(1-t^3\right)\Big)\Big(1+\phi(-t)\Big)\sum_{\substack{x\not\equiv 0,t^{-2}\\ t^{-1},1}} \Big(1+\phi(x)\Big)\Big(1+\phi(1-tx)\Big)\\
&= 2\Big(1+\phi\left(1-t^3\right)\Big)\Big(1+\phi(-t)\Big)\Big(p-8-4\phi(1-t)-\phi(-1)\Big).
\end{aligned}$$

We can use a similar trick in the evaluation of S_3. This shows that

$$\begin{aligned}
S_3 &= \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} 2\Big(1+\phi(y)\Big)\Big(1+\phi(y-t)\Big)\Big(1+\phi(-ty)\Big)\\
&= 2\Big(1+\phi(-t)\Big)\Big(p-9-2\phi(-1)-2\phi(1-t^3)-2\phi(1-t)-\phi(t^2-1)-\phi(1-t^2)\Big).
\end{aligned}$$

The evaluation of S_4 involves the same manipulations as in S_1. These result in

$$\begin{aligned} S_4 &= 2\Big(1+\phi\,(1-t)\Big) \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi\,(y)\Big)\Big(1+\phi\,(y-t)\Big)\Big(1+\phi\,(1-ty)\Big) \\ &= 2\Big(1+\phi\,(1-t)\Big) \Big(p+p_2F_1(t^2)-15-6\phi(-t)-2\phi(t)-2\phi(1+t+t^2) \\ &\qquad -2\phi(-t-t^2-t^3)-2\phi(1+t)-2\phi(t+t^2)\Big). \end{aligned}$$

Likewise, we obtain

$$\begin{aligned} S_5 &= \Big(1+\phi\,(t)\Big) \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi\,(y)\Big)\Big(1+\phi\,(y-t)\Big)\Big(1+\phi\,(1-t^2y)\Big) \\ &= \Big(1+\phi\,(t)\Big) \Big(p+p_2F_1(t^3)-11-4\phi(-1)-4\phi(1-t^3) \\ &\qquad -4\phi(1-t)-4\phi(1+t)-4\phi(1-t^2)\Big). \end{aligned}$$

To evaluate S_6, we simply pull terms to the front and notice a similarity to a previous term. We have

$$\begin{aligned} S_6 &= \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi\,(y)\Big)\Big(1+\phi\,(y-t)\Big)\Big(1+\phi\,(y)\Big)\Big(1+\phi\,(1-ty)\Big)\Big(1+\phi(y)\phi(1-t)\Big) \\ &= 2\Big(1+\phi\,(1-t)\Big) \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi\,(y)\Big)\Big(1+\phi\,(y-t)\Big)\Big(1+\phi\,(1-ty)\Big) \\ &= S_4. \end{aligned}$$

Similarly, we have

$$\begin{aligned} S_7 &= \Big(1+\phi\,(t)\Big) \sum_{\substack{y\not\equiv 0,t^{-2}\\ t^{-1},1,t}} \Big(1+\phi\,(y)\Big)\Big(1+\phi\,(y-t)\Big)\Big(1+\phi\,(1-t^2y)\Big) \\ &= S_5. \end{aligned}$$

Adding this all up, we get

$$\begin{aligned} C_t(p) = \frac{(p-1)}{192}\Big[&90-3p\phi(t)+12\phi(t+t^2)+p^2-14p+48\phi(-t)+27\phi(t)+62\phi(1-t) \\ &+6\phi(1-t^3)+12\phi(t-t^3)+12\phi(1-t^2)+12\phi(-1)+12\phi(1+t)+24\phi(t^2-t) \\ &+6\phi(t-t^4)+12\phi(t-t^2)+3\phi(t^4-t)p-6p\phi(1-t)-3\phi(-t)p+p^2{}_3F_2(t^3) \\ &-6p(1+\phi(1-t))_2F_1(t^2)-3p(1+\phi(t))_2F_1(t^3)\Big], \end{aligned}$$

and this is the desired formula. □

Proof of Corollaries 1 and 2. We begin by stating two well known facts about quadratic residues. First, $\phi(2)$ is 1 when $p \equiv 1$ or $7 \pmod 8$ and -1 when $p \equiv 3$ or $5 \pmod 8$. Second, $\phi(3)$ is 1 when $p = 1$ or $11 \pmod{12}$ and is -1 when $p \equiv 5$ or $7 \pmod{12}$. With these it is simple to show that if $p \equiv 5$ or $7 \pmod{24}$ and $t = -2$ or $p \equiv 7$ or $13 \pmod{24}$

and $t = -1/2$, then $\phi(t) = \phi(1-t) = -1$. When these two facts hold, Theorem 3 simplifies to

$$C_t(p) = \frac{p-1}{192}\Big[p^2 + p^2 {}_3F_2(t^3) - 5p + 3p\phi(-1)\left(1+\phi\left(1+t+t^2\right)\right) + 13 - 12\phi(-1)\Big].$$

The claims follow from the fact that (see [Ono04], pg. 192) for $p \neq 2, 7$ we have

$${}_3F_2(-8) = \begin{cases} -\frac{1}{p} & \text{if } p \equiv 3 \pmod 4, \\ \frac{4x^2-p}{p^2} & \text{if } p \equiv 1 \pmod 4, x^2+y^2 = p, \text{ and } x \text{ odd}, \end{cases}$$

and that for $p \neq 2, 3$ we have

$${}_3F_2\left(\frac{-1}{8}\right) = \begin{cases} -\frac{\phi(2)}{p} & \text{if } p \equiv 3 \pmod 4, \\ \frac{\phi(2)\left(4x^2-p\right)}{p^2} & \text{if } p \equiv 1 \pmod 4, x^2+y^2 = p, \text{ and } x \text{ odd}. \end{cases}$$

Note that we cannot apply these facts in the single case $p = 7$ in Corollary 1. However, it is simple to check by hand that the formula still holds in this case. □

Acknowledgments. This research was supported by the University of Wisconsin-Madison NSF Vigre REU program. The author would like to thank Ken Ono and Jeremy Rouse for their invaluable guidance. The author would also like to thank Karl Mahlburg for his help in proofreading, Sharon Garthwaite for her patience in helping me to use LaTeX, and the referee for numerous helpful suggestions.

References

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR MR1625181 (99d:11092)

[CGW88] F. R. K. Chung, R. L. Graham, and R. M. Wilson, *Quasirandom graphs*, Proc. Nat. Acad. Sci. U.S.A. **85** (1988), no. 4, 969–970. MR MR928566 (89a:05116)

[EPS81] R. J. Evans, J. R. Pulham, and J. Sheehan, *On the number of complete subgraphs contained in certain graphs*, J. Combin. Theory Ser. B **30** (1981), no. 3, 364–371. MR MR624553 (83c:05075)

[Erd62] P. Erdős, *On the number of complete subgraphs contained in certain graphs*, Magyar Tud. Akad. Mat. Kutató Int. Közl. **7** (1962), 459–464. MR MR0151956 (27 #1937)

[Ono04] Ken Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR MR2020489 (2005c:11053)

[Tho97] Andrew Thomason, *Graph products and monochromatic multiplicities*, Combinatorica **17** (1997), no. 1, 125–134. MR MR1466580 (99i:05087)