A conjecture of Evans on Kloosterman sums

Evan P. Dummit, Adam W. Goldberg, and Alexander R. Perry

2009 Wisconsin Number Theory REU Project

Notation

We will make use of the following notation:

- p odd prime
- Additive character $\psi : \mathbb{F}_p \to \mathbb{C},\ x \mapsto e^{\frac{2\pi i x}{p}}$
- $\overline{x} = 1/x$ in $\mathbb{F}_p^\times$
- $\varepsilon : \mathbb{F}_p \to \mathbb{C}, x \mapsto x$
- $\phi : \mathbb{F}_p \to \mathbb{C}, x \mapsto \left(\frac{x}{p}\right)$(Legendre)

Gauss and Jacobi Sums

Definition

For $a \in \mathbb{F}_p$, Quadratic Gauss Sum:

$$G(\phi) := \sum_{a \in \mathbb{F}_p} \phi(a)\psi(a).$$

Gauss and Jacobi Sums

Definition

For $a \in \mathbb{F}_p$, Quadratic Gauss Sum:

$$G(\phi) := \sum_{a \in \mathbb{F}_p} \phi(a)\psi(a).$$

Definition

For multiplicative characters χ_1, χ_2

$$J(\chi_1, \chi_2) := \sum_{a \in \mathbb{F}_p} \chi_1(a)\chi_2(1-a).$$

Kloosterman Sum

Definition

For $a \in \mathbb{F}_p^\times$, the classical Kloosterman sum is

$$K(a) := \sum_{x \in \mathbb{F}_p^\times} \psi(x + a\overline{x}).$$

"Sum" Definitions

Definition

The n-th twisted Kloosterman sheaf of ϕ is

$$T_n := \sum_{a \in \mathbb{F}_p^\times} \phi(a)(g(a)^n + g(a)^{n-1}h(a) + \cdots + h(a)^n),$$

where $g(a)$ and $h(a)$ are the roots of the polynomial

$$X^2 + K(a)X + p.$$

Evans's Conjecture

Define $a(n)$ by

$$\sum_{n=1}^{\infty} a(n)q^n := q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 = q-4q^3-2q^5+24q^7-11q^9-\cdots.$$

Evans's Conjecture

Define $a(n)$ by

$$\sum_{n=1}^{\infty} a(n)q^n := q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 = q-4q^3-2q^5+24q^7-11q^9-\cdots.$$

Conjecture (Evans)

If p is an odd prime, then

$$-\frac{T_4}{p} = a(p).$$

Earlier Related Work

Emma and D. H. Lehmer showed

$$\frac{-\phi(-1)T_3}{p} = \begin{cases} 0 & p \equiv 2 \bmod 3 \\ 4x^2 - 2p & p = x^2 + 3y^2 \end{cases}$$

Earlier Related Work

Emma and D. H. Lehmer showed

$$\frac{-\phi(-1)T_3}{p} = \begin{cases} 0 & p \equiv 2 \bmod 3 \\ 4x^2 - 2p & p = x^2 + 3y^2 \end{cases}$$

These are the values of the p-th coefficients of the eigenform

$$q\prod_{n=1}^{\infty}(1-q^{2n})^3(1-q^{6n})^3 \in S_3\left(\Gamma_0(12), \left(\frac{d}{3}\right)\right).$$

Earlier Related Work, cont.

Green's analogy between character sum expansion of a function $f : \mathbb{F}_p \to \mathbb{C}$ and power series expansion of an analytic function:

$$x^k \leftrightarrow \chi(x).$$

Earlier Related Work, cont.

Green's analogy between character sum expansion of a function $f : \mathbb{F}_p \to \mathbb{C}$ and power series expansion of an analytic function:

$$x^k \leftrightarrow \chi(x).$$

Basis was analogy between the Gauss sum

$$G(\chi) = \sum_{x \in \mathbb{F}_p^\times} \chi(x)\psi(x)$$

Earlier Related Work, cont.

Green's analogy between character sum expansion of a function $f : \mathbb{F}_p \to \mathbb{C}$ and power series expansion of an analytic function:

$$x^k \leftrightarrow \chi(x).$$

Basis was analogy between the Gauss sum

$$G(\chi) = \sum_{x \in \mathbb{F}_p^\times} \chi(x)\psi(x)$$

and the gamma function

$$\Gamma(x) = \int_0^\infty t^x e^{-t} \frac{dt}{t}.$$

Classical Hypergeometric functions

Definition

$$ {}_pF_q\left(\begin{matrix} \alpha_1, & \alpha_2, & \dots & \alpha_p \\ & \beta_1, & \dots & \beta_q \end{matrix} \,\Big|\, x \right) := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n (\alpha_2)_n \cdots (\alpha_p)_n}{(\beta_1)_n \cdots (\beta_q)_n} \frac{x^n}{n!}, $$

Classical Hypergeometric functions

Definition

$$ {}_pF_q\left(\begin{matrix} \alpha_1, & \alpha_2, & \dots\ \alpha_p \\ & \beta_1, & \dots\ \beta_q \end{matrix} \,\middle|\, x \right) := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n (\alpha_2)_n \cdots (\alpha_p)_n}{(\beta_1)_n \cdots (\beta_q)_n} \frac{x^n}{n!}, $$

where $(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1)$.

Gaussian hypergeometric functions I

Definition

For characters A and B on $\mathbb{F}_p$, define the binomial coefficient

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B}) = \frac{B(-1)}{p} \sum_{x \in \mathbb{F}_p} A(x)\overline{B}(1-x).$$

Gaussian hypergeometric functions I

Definition

For characters A and B on $\mathbb{F}_p$, define the binomial coefficient

$$\binom{A}{B} := \frac{B(-1)}{p} J(A, \overline{B}) = \frac{B(-1)}{p} \sum_{x \in \mathbb{F}_p} A(x) \overline{B}(1-x).$$

Definition

For $n \in \mathbb{N}^+$, and $x \in \mathbb{F}_p$, define

$${}_{n+1}F_n(x) := \frac{p}{p-1} \sum_{\chi} \binom{\phi\chi}{\chi}^{n+1} \chi(x).$$

Gaussian hypergeometric functions II

Gaussian hypergeometric functions may in general be written as "Diophantine" sums over $\mathbb{F}_p$.

Gaussian hypergeometric functions II

Gaussian hypergeometric functions may in general be written as "Diophantine" sums over $\mathbb{F}_p$.

Examples:

$$
{}_2F_1(x) = \varepsilon(x)\frac{\phi(-1)}{p}\sum_{y\in\mathbb{F}_p^\times}\phi(y)\phi(1-y)\phi(1-xy),
$$

$$
{}_3F_2(x) = \varepsilon(x)\frac{1}{p^2}\sum_{y,z\in\mathbb{F}_p^\times}\phi(y)\phi(1-y)\phi(z)\phi(1-z)\phi(1-xyz).
$$

Gaussian hypergeometric functions II

Gaussian hypergeometric functions may in general be written as "Diophantine" sums over $\mathbb{F}_p$.
Examples:

$$
{}_2F_1(x) = \varepsilon(x)\frac{\phi(-1)}{p}\sum_{y\in\mathbb{F}_p^\times}\phi(y)\phi(1-y)\phi(1-xy),
$$

$$
{}_3F_2(x) = \varepsilon(x)\frac{1}{p^2}\sum_{y,z\in\mathbb{F}_p^\times}\phi(y)\phi(1-y)\phi(z)\phi(1-z)\phi(1-xyz).
$$

Transformation laws for $x \neq 0,1$:

$$
\begin{aligned}
{}_2F_1(x) &= \phi(-1){}_2F_1(1-x),\\
{}_2F_1(x) &= \phi(x){}_2F_1(\overline{x}).
\end{aligned}
$$

Gaussian hypergeometric functions III

Two other relations:

Gaussian hypergeometric functions III

Two other relations:

Lemma

If $t \neq 0, \pm 1$*, then*

$$ {}_3F_2\left(\frac{1}{1-t^2}\right) = \phi(t^2-1)\left(-\frac{1}{p} + {}_2F_1\left(\frac{1-t}{2}\right)^2\right). $$

Gaussian hypergeometric functions III

Two other relations:

Lemma

If $t \neq 0, \pm 1$, then

$$ {}_3F_2\left(\frac{1}{1-t^2}\right) = \phi(t^2-1)\left(-\frac{1}{p} + {}_2F_1\left(\frac{1-t}{2}\right)^2\right). $$

and

Lemma

$$ p^3 {}_4F_3(1) = p^2 \sum_{x \in \mathbb{F}_p^\times} \phi(x) {}_2F_1(x)^2. $$

Relating geometric objects and counting functions

Ahlgren and Ono proved that

$$p^3 {}_4F_3(1) = -a(p) - p$$

Relating geometric objects and counting functions

Ahlgren and Ono proved that

$$p^3 {}_4F_3(1) = -a(p) - p$$

by showing that the coefficients $a(p)$ and the hypergeometric values $p^3 {}_4F_3(1)$ count points on the "Calabi-Yau" variety

$$\{(x, y, z, w) \in (\mathbb{F}_p^\times)^4 \mid x + \frac{1}{x} + y + \frac{1}{y} + z + \frac{1}{z} + w + \frac{1}{w} = 0\}.$$

Evans's Conjecture reformulated

With this, Evans's conjecture may be rephrased as follows:

Evans's Conjecture reformulated

With this, Evans's conjecture may be rephrased as follows:

Conjecture (Evans)

If p is an odd prime, then

$$\frac{T_4}{p} = p^3 {}_4F_3(1) + p.$$

Twisted moments

Note $g(a)^n + g(a)^{n-1}h(a) + \cdots + g(a)h(a)^{n-1} + h(a)^n \in \mathbb{Z}[K(a)]$.

Twisted moments

Note $g(a)^n + g(a)^{n-1}h(a) + \cdots + g(a)h(a)^{n-1} + h(a)^n \in \mathbb{Z}[K(a)]$. Therefore the m-th moments

$$S(m) = \sum_{a \in \mathbb{F}_p^\times} \phi(a) K(a)^m$$

govern the behavior of the Kloosterman sheaves.

Reductions of $S(m)$

Proposition

For an integer $m \geq 1$, we have that

$$S(m+1) = p\phi(-1) \sum_{x_1,\ldots,x_m \in \mathbb{F}_p^\times} \phi(x_1 + \cdots + x_m + 1)\phi(\overline{x_1} + \cdots + \overline{x_m} + 1).$$

Character Sums I

Definition

For $a, b \in \mathbb{F}_p$,

$$Q(a,b) := \sum_{x,y \in \mathbb{F}_p^\times} \phi(x+y+a)\phi(\overline{x}+\overline{y}+b)$$

Character Sums I

Definition

For $a, b \in \mathbb{F}_p$,

$$Q(a,b) := \sum_{x,y \in \mathbb{F}_p^\times} \phi(x+y+a)\phi(\overline{x}+\overline{y}+b)$$

Proposition

If $a, b \in \mathbb{F}_p^\times$, *then* $Q(a,b) = p^2\phi(-1)\,{}_3F_2\left(\frac{ab}{4}\right) + p\phi(a/b)$.

Character Sums I

Definition

For $a, b \in \mathbb{F}_p$,

$$Q(a,b) := \sum_{x,y \in \mathbb{F}_p^\times} \phi(x+y+a)\phi(\overline{x}+\overline{y}+b)$$

Proposition

If $a, b \in \mathbb{F}_p^\times$, *then* $Q(a,b) = p^2\phi(-1)\,{}_3F_2\left(\frac{ab}{4}\right) + p\phi(a/b)$.

The evaluation of $Q(1,1)$ reduces to yield the Lehmers' result.

Character Sums II

We may now write T_n as sums of ${}_3F_2$'s. For $m \in \mathbb{N}^+$, define

$$G(m) := \sum_{x_1,\ldots,x_m \in \mathbb{F}_p^\times} {}_3F_2\left(\frac{(x_1 + x_2 + \cdots + x_m + 1)(\overline{x_1} + \cdots + \overline{x_m} + 1)}{4}\right).$$

Character Sums II

We may now write T_n as sums of ${}_3F_2$'s. For $m \in \mathbb{N}^+$, define

$$G(m) := \sum_{x_1,\ldots,x_m \in \mathbb{F}_p^\times} {}_3F_2\left(\frac{(x_1 + x_2 + \cdots + x_m + 1)(\overline{x_1} + \cdots + \overline{x_m} + 1)}{4}\right).$$

Theorem

If $n \in \mathbb{N}^+$, then T_n is an explicit linear combination of ${}_3F_2$'s. For $m \geq 1$, there is a recurrence

$$S(m+3) = p^3 G(m) + pS(m+1).$$

Character Sums II

We may now write T_n as sums of ${}_3F_2$'s. For $m \in \mathbb{N}^+$, define

$$G(m) := \sum_{x_1,\ldots,x_m \in \mathbb{F}_p^\times} {}_3F_2\left(\frac{(x_1 + x_2 + \cdots + x_m + 1)(\overline{x_1} + \cdots + \overline{x_m} + 1)}{4}\right).$$

Theorem

If $n \in \mathbb{N}^+$, then T_n is an explicit linear combination of ${}_3F_2$'s. For $m \geq 1$, there is a recurrence

$$S(m+3) = p^3 G(m) + pS(m+1).$$

Character Sums III

Lemma

For $F : \mathbb{F}_p^\times \to \mathbb{C}$ defined by

$$F(a) := Q(a+1, \overline{a}+1),$$

we have

$$T_4 = p\phi(-1) \sum_{x \in \mathbb{F}_p^\times} F(x) + 3p^2.$$

Character Sums IV: A New Hope

Lemma

For $a \neq \pm 1$, we have that

$$F(a) = p^2 \phi(a)_2 F_1(-a)^2.$$

Character Sums IV: A New Hope

Lemma

For $a \neq \pm 1$, we have that

$$F(a) = p^2 \phi(a) {}_2F_1(-a)^2.$$

Lemma

We have that

$$\phi(-1)F(1) = p^2 \phi(-1) {}_2F_1(-1)^2 - p$$
$$\phi(-1)F(-1) = p^2 {}_2F_1(1)^2 - p$$

Apéry numbers I

Definition

The Apéry numbers are defined by

$$A(n) := \sum_{j=0}^{n} \binom{n+j}{j}^2 \binom{n}{j}^2.$$

Apéry numbers I

Definition

The Apéry numbers are defined by

$$A(n) := \sum_{j=0}^{n} \binom{n+j}{j}^2 \binom{n}{j}^2 .$$

They were used in the famous proof that $\zeta(3)$ is irrational.

Apéry numbers II

Let

$$\sum_{n=1}^{\infty} a(n)q^n := q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 = q-4q^3-2q^5+24q^7-11q^9-\cdots .$$

Apéry numbers II

Let

$$\sum_{n=1}^{\infty} a(n)q^n := q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 = q-4q^3-2q^5+24q^7-11q^9-\cdots.$$

Conjecture (Beukers)

$$A\left(\frac{p-1}{2}\right) \equiv a(p) \bmod p^2.$$

Apéry numbers II

Let

$$\sum_{n=1}^{\infty} a(n)q^n := q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4 = q-4q^3-2q^5+24q^7-11q^9-\cdots .$$

Conjecture (Beukers)

$$A\left(\frac{p-1}{2}\right) \equiv a(p) \bmod p^2.$$

This was proven by Ahlgren and Ono using the combinatorial properties of ${}_4F_3(1)$ and the relation $p^3\,{}_4F_3(1) = -a(p) - p$.

Beukers-type congruences for T_n

Definition

For $\lambda \in \mathbb{F}_p$, define the generalized Apéry number by

$$A(p,\lambda) := \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 \binom{\frac{p-1}{2}+j}{j} \lambda^{pj}.$$

Beukers-type congruences for T_n

Definition

For $\lambda \in \mathbb{F}_p$, define the generalized Apéry number by

$$A(p,\lambda) := \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 \binom{\frac{p-1}{2}+j}{j} \lambda^{pj}.$$

Theorem

If n is a positive integer, then modulo p^2, T_{n+3} equals

$$(-1)^{n+1} p \sum_{x_1,\ldots,x_n \in \mathbb{F}_p^\times} A\left(p, \frac{(x_1+\cdots+x_n+1)(\overline{x_1}+\cdots+\overline{x_n}+1)}{4}\right).$$

Conclusion

- Proved Evans's Conjecture
- Expanded on the work of the Lehmer's with Q(a,b)
- Apéry number observations

Conclusion

Theorem (DGP)

Evans's Conjecture is true, namely If p is an odd prime, then

$$-\frac{T_4}{p} = a(p).$$

Conclusion

Theorem (DGP)

Evans's Conjecture is true, namely If p is an odd prime, then

$$-\frac{T_4}{p} = a(p).$$

Theorem

If n is a positive integer, then modulo p^2, T_{n+3} equals

$$(-1)^{n+1} p \sum_{x_1,\ldots,x_n \in \mathbb{F}_p^\times} A\left(p, \frac{(x_1 + \cdots + x_n + 1)(\overline{x_1} + \cdots + \overline{x_n} + 1)}{4}\right).$$