GAUSS SUMS

BOGDAN NICA

> *Comme quelqu'un pourrait dire de moi, que j'ai seulement fait ici un amas de fleurs étrangères: n'y ayant fourni du mien, que le filet à les lier.* (Michel de Montaigne, *Essais*)

This is an essay on Gauss sums and some of their applications.

In the first part we consider quadratic Gauss sums of odd order, the core result being the evaluation of these sums. This turns out to be a by-product of a different question, of independent interest: that of finding the eigenvalues of the Fourier matrix. As applications, we prove the law of quadratic reciprocity, we derive some elementary but non-trivial trigonometric identities, and we discuss the diagonalization of the Jacobsthal matrix.

In the second part, we consider more general Gauss sums, but only of prime order. Here the viewpoint is more algebraic; to begin with, we need the character theory of finite abelian groups. Gauss sums cannot be evaluated, in general, beyond their absolute value. This fact is already very useful; we use it to estimate some character sums–notably, we prove the Pólya–Vinogradov inequality. We also use Gauss sums to diagonalize the Fourier matrix of prime order.

Contents

Date: December 12, 2023.

1. Quadratic Gauss sums

1.1. **Roots of unity.** Let

$$\zeta_n = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$$

denote the 'first' n-th root of unity in $\mathbb{C}^*$. Since ζ_n has multiplicative order n, it follows that

$$\sum_{k=0}^{n-1} \zeta_n^{rk} = \begin{cases} n & \text{if } n \mid r, \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

In turn, this implies–by a calculation left to the reader–the following fact.

Lemma 1.1. *For any choice of* $a_0, \dots, a_{n-1} \in \mathbb{C}$*, we have*

$$\sum_{k=0}^{n-1} \Big| \sum_{j=0}^{n-1} a_j \zeta_n^{jk} \Big|^2 = n \sum_{k=0}^{n-1} |a_k|^2. \tag{2}$$

As a concrete instance of (2), we record the following identity. Here, and throughout these notes, $|A|$ denotes the cardinality of a finite set A.

Corollary 1.2. *Let* $A \subseteq \{0, \dots, n-1\}$. *Then*

$$\sum_{k=0}^{n-1} \Big| \sum_{j\in A} \zeta_n^{jk} \Big|^2 = n|A|. \tag{3}$$

Application 1.3. Consider two subsets $A, B \subseteq \{0, \dots, n-1\}$. We claim that

$$\Big| \sum_{a\in A} \sum_{b\in B} \zeta_n^{ab} \Big| \leq \sqrt{n|A||B|}. \tag{4}$$

Indeed, we have

$$\Big| \sum_{a\in A} \sum_{b\in B} \zeta_n^{ab} \Big| \leq \sum_{a\in A} \Big| \sum_{b\in B} \zeta_n^{ab} \Big| \leq \sqrt{|A| \sum_{a\in A} \Big| \sum_{b\in B} \zeta_n^{ab} \Big|^2}$$

by the Cauchy-Schwarz inequality. Next, by (3) we have

$$\sum_{a\in A} \Big| \sum_{b\in B} \zeta_n^{ab} \Big|^2 \leq \sum_{a=0}^{n-1} \Big| \sum_{b\in B} \zeta_n^{ab} \Big|^2 = n|B|.$$

By combining the two inequalities we obtain (4).

By reading off the real and the imaginary part, (4) implies the following inequalities for partial trigonometric sums:

$$\Big| \sum_{a\in A} \sum_{b\in B} \cos\left(\frac{2\pi ab}{n}\right) \Big| \leq \sqrt{n|A||B|},$$

$$\Big| \sum_{a\in A} \sum_{b\in B} \sin\left(\frac{2\pi ab}{n}\right) \Big| \leq \sqrt{n|A||B|}.$$

These seemingly elementary inequalities are remarkably non-trivial when taken out of the context we have just described.

1.2. **The Fourier matrix.** The *Fourier matrix* of order n is the symmetric matrix

$$F_n = \left(\zeta_n^{rs}\right)_{0\leq r,s\leq n-1}.$$

For instance

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \zeta_4 & \zeta_4^2 & \zeta_4^3 \\ 1 & \zeta_4^2 & \zeta_4^4 & \zeta_4^6 \\ 1 & \zeta_4^3 & \zeta_4^6 & \zeta_4^9 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Using (1), it is easy to see that

$$F_n F_n^* = F_n^* F_n = nI_n. \tag{5}$$

On the one hand, (5) says that the normalized Fourier matrix $F_n/\sqrt{n}$ is unitary. On the other hand, (5) implies that the eigenvalues of F_n have absolute value $\sqrt{n}$. Going beyond this quick fact, we aim to find the eigenvalues of F_n together with their multiplicities.

Theorem 1.4. *The eigenvalues of F_n, and their multiplicities, are as follows:*

eigenvalue	$\sqrt{n}$	$-\sqrt{n}$	$i\sqrt{n}$	$-i\sqrt{n}$
multiplicity	$\lfloor (n+4)/4 \rfloor$	$\lfloor (n+2)/4 \rfloor$	$\lfloor (n+1)/4 \rfloor$	$\lfloor (n-1)/4 \rfloor$

It turns out that the multiplicity of each eigenvalue is roughly $n/4$.

Herein, we prove Theorem 1.4 in the case when n is odd. This case suffices for our purposes. The reader is invited to prove Theorem 1.4 in the case when n is even, by adapting the arguments given below.

We start with two preliminary facts about the trace and the determinant of F_n.

Lemma 1.5. *Let n be odd. Then $|\mathrm{Tr}(F_n)| = \sqrt{n}$.*

Proof. We have

$$\mathrm{Tr}(F_n) = \sum_{r=0}^{n-1} \zeta_n^{r^2}$$

and so

$$|\mathrm{Tr}(F_n)|^2 = \mathrm{Tr}(F_n)\cdot\overline{\mathrm{Tr}(F_n)} = \sum_{r=0}^{n-1}\sum_{s=0}^{n-1} \zeta_n^{r^2-s^2}.$$

We make the change of variable $s := s - r$, understood modulo n, in the inner sum; then we interchange the order of summation:

$$|\mathrm{Tr}(F_n)|^2 = \sum_{s=0}^{n-1} \zeta_n^{-s^2} \sum_{r=0}^{n-1} \zeta_n^{2sr}.$$

By (1), the inner sum vanishes except when n divides $2s$, in which case it equals n. As n is odd, n divides $2s$ precisely when n divides s; in the range $s \in \{0, \dots, n-1\}$, this happens for $s = 0$ only. We conclude that $|\mathrm{Tr}(F_n)|^2 = n$. □

Lemma 1.6. *Let n be odd. Then* $\det(F_n)$ *is a positive multiple of* $(-i)^{(n-1)/2}$.

Proof. Since F_n is a Vandermonde matrix, we have

$$\det(F_n) = \prod_{r<s} (\zeta_n^s - \zeta_n^r)$$

where, we recall, r and s take values in $\{0, \dots, n-1\}$. We rewrite each factor of the product as follows:

$$\zeta_n^s - \zeta_n^r = \zeta_{2n}^{r+s}\big(\zeta_{2n}^{s-r} - \zeta_{2n}^{-(s-r)}\big) = \zeta_{2n}^{r+s} \cdot 2i \sin \frac{(s-r)\pi}{n}.$$

Note that $(s-r)\pi/n \in (0, \pi)$, since $0 \leq r < s \leq n-1$, and so the sine factor on the right-hand side is positive. Thus, for some $C > 0$ we have

$$\det(F_n) = C \prod_{r<s} i\, \zeta_{2n}^{r+s} = C i^{n(n-1)/2} \prod_{r<s} \zeta_{2n}^{r+s}.$$

As n is odd, we have $i^{n(n-1)/2} = (-i)^{(n-1)/2}$. Also, the latter product in the formula displayed above equals 1; indeed, the exponent of ζ_{2n} is

$$\begin{aligned}\sum_{r<s}(r+s) &= \frac{1}{2}\Big(\sum_{r,s}(r+s) - \sum_{r=s}(r+s)\Big)\\ &= \frac{2n-2}{2}\Big(\sum_r r\Big) = 2n\Big(\frac{n-1}{2}\Big)^2,\end{aligned}$$

which is a multiple of $2n$. □

Proof of Theorem 1.4 when n is odd. As already pointed out, the eigenvalues of F_n have modulus $\sqrt{n}$. Our aim is to determine the multiplicities of the possible eigenvalues $\pm\sqrt{n}$, $\pm i\sqrt{n}$. We denote them as follows:

- m_+ and m_- are the multiplicities of $\sqrt{n}$ respectively $-\sqrt{n}$;
- m'_+ and m'_- are the multiplicities of $i\sqrt{n}$ respectively $-i\sqrt{n}$.

The spectral picture of F_n simplifies upon squaring: F_n^2 can only have eigenvalues n and $-n$, while F_n^4 can only have one eigenvalue, n.

Indeed, the matrix F_n^2 turns out to be far simpler than F_n. Its (r, s) entry is

$$\sum_{k=0}^{n-1} \zeta_n^{rk} \cdot \zeta_n^{ks} = \sum_{k=0}^{n-1} \zeta_n^{(r+s)k} = \begin{cases} n & \text{if } n \mid r+s \\ 0 & \text{otherwise} \end{cases}$$

by (1). For $r, s \in \{0, \dots, n-1\}$, we have that $r+s$ is a multiple of n if and only if $r = s = 0$, or $r + s = n$. Thus $F_n^2 = nC$ where C is the n-by-n matrix

$$C = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ & & \dots & & \\ 0 & 1 & \dots & 0 & 0 \end{pmatrix}.$$

Taking a further step, we notice that $C^2 = I_n$. The eigenvalues of C can now be easily determined. They are ± 1, and they sum up to $\mathrm{Tr}(C) = 1$; the latter formula owes to n being odd. It follows that the eigenvalues of C are 1 with multiplicity $\frac{1}{2}(n+1)$, respectively -1 with multiplicity $\frac{1}{2}(n-1)$.

There are two direct consequences concerning F_n. The first one, not needed in what follows but too pretty to go unnoticed, is that $F_n^4 = n^2 I_n$; in other words, the normalized Fourier matrix $F_n/\sqrt{n}$ has order 4. The second consequence addresses our main interest, the eigenvalue multiplicities for F_n. As F_n^2 has eigenvalues n, with multiplicity $\frac{1}{2}(n+1)$, and $-n$, with multiplicity $\frac{1}{2}(n-1)$, we deduce that

$$m_+ + m_- = \tfrac{1}{2}(n+1), \qquad m'_+ + m'_- = \tfrac{1}{2}(n-1). \tag{6}$$

Additional spectral information can be found in the trace and the determinant of F_n. It is at this point that we bring in the preliminary lemmas.

As

$$\begin{aligned} \mathrm{Tr}(F_n) &= m_+\sqrt{n} + m_-(-\sqrt{n}) + m'_+ i\sqrt{n} + m'_-(-i\sqrt{n}) \\ &= \big((m_+ - m_-) + (m'_+ - m'_-)i\big)\sqrt{n}, \end{aligned}$$

knowing that $|\mathrm{Tr}(F_n)| = \sqrt{n}$ forces one of the following to hold:

$$\begin{cases} m_+ - m_- = \pm 1 \\ m'_+ - m'_- = 0 \end{cases} \quad \text{or} \quad \begin{cases} m_+ - m_- = 0 \\ m'_+ - m'_- = \pm 1 \end{cases}. \tag{7}$$

On the other hand, we have

$$\begin{aligned} \det(F_n) &= (\sqrt{n})^{m_+} \cdot (-\sqrt{n})^{m_-} \cdot (i\sqrt{n})^{m'_+} \cdot (-i\sqrt{n})^{m'_-} \\ &= (-1)^{m_- - m'_+} \cdot (-i)^{(n-1)/2} \cdot \sqrt{n}^{\,n} \end{aligned}$$

since $m'_+ + m'_- = \frac{1}{2}(n-1)$. For $\det(F_n)$ to be a positive multiple of $(-i)^{(n-1)/2}$, we must have

$$m_- \equiv m'_+ \mod 2. \tag{8}$$

The combination of (6), (7), (8) allows us to deduce the eigenvalue multiplicities. If $n \equiv 1$ mod 4, say $n = 4u+1$, then $m'_+ = m'_- = m_- = u$ and $m_+ = u+1$. If $n \equiv 3$ mod 4, say $n = 4v+3$, then $m_+ = m_- = m'_+ = v+1$ and $m'_- = v$. In either case,

$$m'_+ = m_- = \lfloor (n+1)/4 \rfloor, \quad m'_- = \lfloor n/4 \rfloor, \quad m_+ = \lfloor n/4 \rfloor + 1.$$

This completes the proof. □

Notes. The *discrete Fourier transform* maps a vector $a = (a_0, \dots, a_{n-1}) \in \mathbb{C}^n$ to the vector $\hat{a} = (\hat{a}_0, \dots, \hat{a}_{n-1}) \in \mathbb{C}^n$, where

$$\hat{a}_k = \sum_{j=0}^{n-1} a_j \zeta_n^{jk}.$$

The discrete Fourier transform is an invertible linear map, whose matrix representation in the standard basis of $\mathbb{C}^n$ is the Fourier matrix F_n. In this context, formula (2) says that $\|\hat{a}\|_2 = \sqrt{n}\,\|a\|_2$.

1.3. **Quadratic Gauss sums.** The *quadratic Gauss sum* of order n is the sum

$$\Gamma_n = \sum_{k=0}^{n-1} \zeta_n^{k^2}.$$

With the Fourier matrix in mind, we recognize that $\Gamma_n = \mathrm{Tr}(F_n)$. Since we know the complete spectrum of F_n, thanks to Theorem 1.4, the following explicit computation is immediate.

Theorem 1.7. *Let n be odd. Then*

$$\Gamma_n = \begin{cases} \sqrt{n} & \textit{if } n \equiv 1 \textit{ mod } 4, \\ i\sqrt{n} & \textit{if } n \equiv 3 \textit{ mod } 4. \end{cases}$$

Once again, herein we are only interested in the case when n is odd. For the record, however, let us spell out the explicit evaluation of the quadratic Gauss sum of even order:

$$\Gamma_n = \begin{cases} 0 & \text{if } n \equiv 2 \text{ mod } 4, \\ (1+i)\sqrt{n} & \text{if } n \equiv 0 \text{ mod } 4. \end{cases}$$

Particularly interesting is the case when the order is prime. In Lemma 1.9 below, we give an alternate formula for a quadratic Gauss sum of prime order as a signed summation involving *all* the roots of unity, the signing being given by the Legendre symbol.

Let p be an odd prime. The *Legendre symbol* records the quadratic nature modulo p of a given integer, as follows. When a is a multiple of p, we set $(a/_p) = 0$. For a relatively prime to p, we set

$$(a/_p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Here, an integer a relatively prime to p is said to be a quadratic residue mod p if the equation $x^2 \equiv a$ mod p is solvable; otherwise, a is a quadratic non-residue. Elaborating further, we note the following: for each integer a, the number of solutions $x \in \{0, 1, \dots, p-1\}$ to the equation $x^2 \equiv a$ mod p is $1 + (a/_p)$.

We recall a few fundamental facts about the Legendre symbol. Firstly, it is periodic: if $a \equiv b$ mod p, then $(a/_p) = (b/_p)$. The upshot is that we can restrict to the modular interval $\{0, 1, \dots, p-1\} \subseteq \mathbb{Z}$, or we can induce a map on the quotient $\mathbb{Z}/p\mathbb{Z}$, whenever convenient.

Secondly, the Legendre symbol is multiplicative: for any two integers a and b, we have

$$({}^{a}\!/_{p})({}^{b}\!/_{p}) = ({}^{ab}\!/_{p}).$$

One way to to obtain this is by means of the Euler formula $a^{(p-1)/2} \equiv ({}^{a}\!/_{p})$ mod p. This formula also gives the useful fact that

$$({}^{-1}\!/_{p}) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4, \\ -1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Thirdly, the Legendre symbol is balanced: there are as many quadratic residues mod p as quadratic non-residues mod p in $\{1, \dots, p-1\}$; namely, $(p-1)/2$ of each kind. This can be stated as follows.

Lemma 1.8. *We have*

$$\sum_{k=0}^{p-1} ({}^{k}\!/_{p}) = 0.$$

Proof. Consider the squaring map $s : \{0, 1, \dots, p-1\} \to \{0, 1, \dots, p-1\}$, given by $s(x) = x^2$ mod p. For each $k = 0, \dots, p-1$, the preimage $s^{-1}(k)$ has $1 + ({}^{k}\!/_{p})$ elements. Therefore

$$p = \sum_{k=0}^{p-1} |s^{-1}(k)| = \sum_{k=0}^{p-1} \big(1 + ({}^{k}\!/_{p})\big) = p + \sum_{k=0}^{p-1} ({}^{k}\!/_{p}),$$

and the claimed identity follows. □

After this brief interlude on the Legendre symbol, let us return to quadratic Gauss sums.

Lemma 1.9. *Let p be an odd prime. Then*

$$\Gamma_p = \sum_{k=0}^{p-1} ({}^{k}\!/_{p})\, \zeta_p^k.$$

Proof. We continue using the squaring map introduced in the proof of the previous lemma. We have

$$\begin{aligned} \Gamma_p &= \sum_{j=0}^{p-1} \zeta_p^{j^2} = \sum_{j=0}^{p-1} \zeta_p^{s(j)} = \sum_{k=0}^{p-1} |s^{-1}(k)|\, \zeta_p^k \\ &= \sum_{k=0}^{p-1} \big(1 + ({}^{k}\!/_{p})\big)\zeta_p^k = \sum_{k=0}^{p-1} ({}^{k}\!/_{p})\, \zeta_p^k \end{aligned}$$

since $\sum_{k=0}^{p-1} \zeta_p^k = 0$. □

The above lemma is a very useful observation. It is the starting point for defining general Gauss sums, which we will treat in some detail later on.

Notes. Quadratic Gauss sums were first introduced end evaluated by Gauss. It is very easy to compute the absolute size of a quadratic Gauss sum; this is what Lemma 1.5 does. But the matter of actually evaluating the quadratic Gauss sums is decidedly non-trivial. It took Gauss four years to settle this evaluation. In August 1805, he wrote the following in his mathematical diary:

> *Demonstratio theorematis venustissimi supra 1801 Mai commemorati, quam per 4 annos et ultra omni contentione quaesiveramus, tandem perfecimus.* (The proof of the most beautiful theorem mentioned above, May 1801, which we had been seeking for 4 years and more with all efforts, we have at last completed.)

Gauss's original approach to the evaluation of quadratic Gauss sums used what are now called Gaussian, or q-binomial coefficients. For an in-depth analysis of this particular spot in the wide-ranging work of Gauss, we refer to the superb account of Patterson [15].

The elegant approach via the Fourier matrix, adopted herein, is due to Schur [18]. The Fourier matrix is a distinguished matrix, underlying the discrete Fourier transform, so Theorem 1.7 is of independent interest.

1.4. **Quadratic reciprocity.** The law of quadratic reciprocity exhibits a correlation between the Legendre symbols for two distinct primes. This is unexpected, because we usually think of distinct primes as being arithmetically independent.

Theorem 1.10. *Let p and q be distinct odd primes. Then*

$$({}^{q}\!/_{p}) = \epsilon_{pq}\,({}^{p}\!/_{q})$$

where

$$\epsilon_{pq} = (-1)^{(p-1)(q-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ mod } 4 \text{ or } q \equiv 1 \text{ mod } 4, \\ -1 & \text{if } p \equiv 3 \text{ mod } 4 \text{ and } q \equiv 3 \text{ mod } 4. \end{cases}$$

We will obtain the law of quadratic reciprocity from the following product relation for quadratic Gauss sums.

Lemma 1.11. *Let p and q be distinct odd primes. Then*

$$\Gamma_{pq} = ({}^{q}\!/_{p})\,({}^{p}\!/_{q})\,\Gamma_p\,\Gamma_q.$$

Proof. We have

$$\Gamma_p = \sum_{k=0}^{p-1} ({}^{k}\!/_{p})\,\zeta_p^k = \sum_{k=0}^{p-1} ({}^{qk}\!/_{p})\,\zeta_p^{qk}$$

since $k \mapsto qk$ mod p permutes $\{0, 1, \ldots, p-1\}$. Thanks to the multiplicativity of the Legendre symbol, we deduce that

$$({}^{q}\!/_{p})\,\Gamma_p = \sum_{k=0}^{p-1} ({}^{k}\!/_{p})\,\zeta_p^{qk}.$$

Note, at this point, that the argument of Lemma 1.9 is valid for any p-th root of unity, so we may use ζ_p^q in place of ζ_p to deduce that

$$(q/_p)\,\Gamma_p = \sum_{k=0}^{p-1} (\zeta_p^q)^{k^2} = \sum_{k=0}^{p-1} \zeta_{pq}^{(qk)^2}.$$

There is, of course, a similar formula for $(p/_q)\,\Gamma_q$. Multiplying the two formulas we get

$$\begin{aligned}(q/_p)\,(p/_q)\,\Gamma_p\,\Gamma_q &= \Bigg(\sum_{k=0}^{p-1} \zeta_{pq}^{(qk)^2}\Bigg)\Bigg(\sum_{j=0}^{q-1} \zeta_{pq}^{(pj)^2}\Bigg)\\ &= \sum_{k=0}^{p-1}\sum_{j=0}^{q-1} \zeta_{pq}^{(qk)^2+(pj)^2} = \sum_{k=0}^{p-1}\sum_{j=0}^{q-1} \zeta_{pq}^{(qk+pj)^2}.\end{aligned}$$

But $\{qk + pj : k = 0, \ldots, p-1;\ j = 0, \ldots, q-1\} = \{0, 1, \ldots, pq-1\}$, so the latter sum is precisely Γ_{pq}. □

Proof of Theorem 1.10. The previous lemma gives

$$(q/_p)\,(p/_q) = \frac{\Gamma_{pq}}{\Gamma_p\,\Gamma_q}.$$

Thanks to Theorem 1.7, we can compute the right-hand ratio: if $p, q \equiv 1 \bmod 4$, it equals 1; if $p, q \equiv 3 \bmod 4$, it equals -1; if $p \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$, or vice versa, then it equals 1. In summary, the right-hand ratio is precisely the signing ϵ_{pq} described in the statement. The claimed formula follows by rearranging. □

Notes. Although quadratic Gauss sums first arose in a different context, Gauss soon saw how to use them in order to prove the quadratic reciprocity law. This is neither the first nor the last proof of the quadratic reciprocity law that Gauss found. Gauss's quest for several different proofs attest to his fascination with this somewhat mysterious law.

After Gauss, many other proofs of the quadratic reciprocity law have been found. This is, then, a proper ground for testing a philosophical question: what is a *good* proof? For a nice discussion of depth versus transparency in various approaches to the quadratic reciprocity law, see D'Alessandro [4].

1.5. **Some trigonometric identities.** We now turn to illustrating the use of quadratic Gauss sums in the quaint art of trigonometry. Indeed, a quadratic Gauss sum is, in essence, a trigonometric-type sum:

$$\Gamma_n = \sum_{k=0}^{n-1} \zeta_n^{k^2} = 1 + \sum_{k=1}^{n-1} \cos\left(\frac{2\pi k^2}{n}\right) + i\sum_{k=1}^{n-1} \sin\left(\frac{2\pi k^2}{n}\right)$$

The evaluation of quadratic Gauss sums, given in Theorem 1.7, can therefore be stated in purely trigonometric terms.

Theorem 1.12. *Let n be odd. Then*

$$\sum_{k=1}^{n-1} \cos\left(\frac{2\pi k^2}{n}\right) = \begin{cases} \sqrt{n}-1 & \textit{if } n \equiv 1 \textit{ mod } 4, \\ -1 & \textit{if } n \equiv 3 \textit{ mod } 4 \end{cases} \tag{9}$$

and

$$\sum_{k=1}^{n-1} \sin\left(\frac{2\pi k^2}{n}\right) = \begin{cases} 0 & \textit{if } n \equiv 1 \textit{ mod } 4, \\ \sqrt{n} & \textit{if } n \equiv 3 \textit{ mod } 4 \end{cases} \tag{10}$$

We continue focusing on the case when n is odd, but we remind the reader that related formulas can also be written down when n is even.

Out of the above formulas (9) and (10) flow a number of concrete trigonometric identities. They typically arise for small values of n, and that makes them decidedly deceptive–they look elementary enough, yet they are quite non-trivial without the background offered by quadratic Gauss sums.

Example 1.13. We have

$$\cos\left(\frac{2\pi}{17}\right) + \cos\left(\frac{4\pi}{17}\right) + \cos\left(\frac{8\pi}{17}\right) + \cos\left(\frac{16\pi}{17}\right) = \frac{\sqrt{17}-1}{4}.$$

This follows by using (9) for $n = 17$. The squares modulo 17 are $\pm 1, \pm 2, \pm 4, \pm 8$. So each term $\cos(2k\pi/17)$, where $k = 1, 2, 4, 8$, appears four times on the left-hand side of (9).

Example 1.14. We show that

$$\tan\left(\frac{3\pi}{11}\right) + 4\sin\left(\frac{2\pi}{11}\right) = \sqrt{11}.$$

We aim to exploit (10) for $n = 11$. Put $\theta = \pi/11$. The squares modulo 11 are $1, -2, 3, 4, 5$, so we have

$$\sin(2\theta) - \sin(4\theta) + \sin(6\theta) + \sin(8\theta) + \sin(10\theta) = \frac{\sqrt{11}}{2}.$$

We pack all the arguments into $[0, \pi/2]$ by using the symmetry $\sin(\pi - x) = \sin x$:

$$\sin(\theta) + \sin(2\theta) + \sin(3\theta) - \sin(4\theta) + \sin(5\theta) = \frac{\sqrt{11}}{2}.$$

We now posit an identity of the form

$$\tan(3\theta) = 2\sum_{k=1}^{5} c_k \sin(k\theta).$$

Multiplying through by $\cos(3\theta)$, and using the formula $2\cos x \sin y = \sin(y-x) + \sin(y+x)$, we turn the above identity into

$$\sin(3\theta) = \sum_{k=1}^{5} c_k \sin\big((k-3)\theta\big) + \sum_{k=1}^{5} c_k \sin\big((k+3)\theta\big).$$

The right-hand side can be put in the form

$$a_1 \sin(\theta) + a_2 \sin(2\theta) + a_3 \sin(3\theta) + a_4 \sin(4\theta) + a_5 \sin(5\theta)$$

by using the formulas $\sin(\pi - x) = \sin x$ and $\sin(-x) = -\sin x$. The coefficients are easily found: $a_1 = c_4 - c_2$, $a_2 = c_5 - c_1$, $a_3 = c_5$, $a_4 = c_1 + c_4$, and $a_5 = c_2 + c_3$. So we do have an identity if we impose $a_1 = a_2 = a_4 = a_5 = 0$ and $a_3 = 1$. This leads us to the alternating coefficients $c_1 = c_3 = c_5 = 1$ and $c_2 = c_4 = -1$.

We thus find that

$$\begin{aligned}\frac{1}{2}\tan(3\theta) &= \sin(\theta) - \sin(2\theta) + \sin(3\theta) - \sin(4\theta) + \sin(5\theta)\\ &= \frac{\sqrt{11}}{2} - 2\sin(2\theta).\end{aligned}$$

The claimed formula follows by rearranging.

Notes. The evaluation of

$$\cos\left(\frac{2\pi}{13}\right) + \cos\left(\frac{6\pi}{13}\right) + \cos\left(\frac{8\pi}{13}\right)$$

is the starting point for Sury's nice piece [19]. By an argument just like the one given in Example 1.13, the answer turns out to be $(\sqrt{13} - 1)/2$. Sury goes on to discuss quadratic Gauss sums and their evaluation. He follows the same approach as the one presented herein–namely, Schur's argument using the Fourier matrix.

For a more elaborate discussion of Example 1.14, and kindred identities, see Moll [12].

1.6. **The Jacobsthal matrix.** The *Jacobsthal matrix* of order p is the matrix

$$Q_p = \big((a - b/p)\big)_{0 \le a,b \le p-1}.$$

Thus Q_p has 1 or -1 as off-diagonal entries, respectively 0 along the diagonal. For example:

$$Q_5 = \begin{pmatrix} 0 & 1 & -1 & -1 & 1\\ 1 & 0 & 1 & -1 & -1\\ -1 & 1 & 0 & 1 & -1\\ -1 & -1 & 1 & 0 & 1\\ 1 & -1 & -1 & 1 & 0 \end{pmatrix},$$

and

$$Q_7 = \begin{pmatrix} 0 & -1 & -1 & 1 & -1 & 1 & 1\\ 1 & 0 & -1 & -1 & 1 & -1 & 1\\ 1 & 1 & 0 & -1 & -1 & 1 & -1\\ -1 & 1 & 1 & 0 & -1 & -1 & 1\\ 1 & -1 & 1 & 1 & 0 & -1 & -1\\ -1 & 1 & -1 & 1 & 1 & 0 & -1\\ -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{pmatrix}.$$

We observe the following properties of the Jacobsthal matrix:

- Q_p is circulant: a cyclic shift of a row (or column) yields the next row (respectively, the next column);
- each row and each column of Q_p sums up to 0;
- Q_p is symmetric for $p \equiv 1 \bmod 4$, respectively antisymmetric for $p \equiv 3 \bmod 4$.

Another key property of the Jacobsthal matrix is that

$$Q_p^2 = (-1/_p)\,(pI_p - J_p)$$

where I_p is the identity matrix of order p, and J_p is the all-1 matrix of order p. This is a direct consequence of the following convolution-type computation for the Legendre symbol.

Lemma 1.15. *Let a and b be integers. Then*

$$\sum_{c=0}^{p-1} (a-c/_p)\,(c-b/_p) = \begin{cases} -(-1/_p) & \textit{if } a \not\equiv b \textit{ mod } p,\\ (-1/_p)\,(p-1) & \textit{if } a \equiv b \textit{ mod } p. \end{cases}$$

Proof. We write

$$\begin{aligned}\sum_{c=0}^{p-1} (a-c/_p)\,(c-b/_p) &= (-1/_p)\sum_{c=0}^{p-1} (c-a/_p)\,(c-b/_p)\\ &= (-1/_p)\sum_{c=0}^{p-1} \big(c(c+a-b)/_p\big)\end{aligned}$$

by using the multiplicativity of the Legendre symbol, followed by the reindexing $c := c + a$. It therefore suffices to prove that, whenever d is an integer, we have

$$\sum_{k=0}^{p-1} \big(k(k+d)/_p\big) = \begin{cases} -1 & \text{if } d \not\equiv 0 \text{ mod } p,\\ p-1 & \text{if } d \equiv 0 \text{ mod } p. \end{cases}$$

The case $d \equiv 0 \bmod p$ is obvious, as $(k^2/_p) = 1$ for all $k = 1, \dots, p-1$. Assume $d \not\equiv 0 \bmod p$ in what follows. Note that we can still drop the index value $k = 0$ from the sum. For each $k \in \{1 \dots, p-1\}$ there exists a unique $k' \in \{1 \dots, p-1\}$ such that $kk' \equiv 1 \bmod p$; thus k' is the modular inverse of k. As $(kk'/_p) = (1/_p) = 1$, we have $(k/_p) = (k'/_p)$. We deduce that

$$\sum_{k=0}^{p-1} \big(k(k+d)/_p\big) = \sum_{k=1}^{p-1} \big(k'(k+d)/_p\big).$$

Consider the map $f : \{1, \dots, p-1\} \to \{0, 1, \dots, p-1\}$ given by $k \mapsto k'(k+d) \bmod p$. The key point is that f is one-to-one. Indeed, assume $k_1, k_2 \in \{1, \dots, p-1\}$ satisfy $k_1'(k_1+d) \equiv k_2'(k_2+d) \bmod p$. Then $k_2(k_1+d) \equiv k_1(k_2+d) \bmod p$ and so $k_2 d \equiv k_1 d \bmod p$. As d is relatively prime to p, it follows that k_2 and k_1 are congruent modulo p, whence equal.

We infer that the map f misses exactly one value in its codomain $\{0, 1, \dots, p-1\}$. It is not hard to guess that the unattained value is 1; for $k'(k+d) \equiv 1 \bmod p$ would imply $k + d \equiv k \bmod p$, whence $d \equiv 0 \bmod p$–a contradiction.

In light of Lemma 1.8, we deduce that

$$\sum_{k=1}^{p-1} \big(k'(k+d)/_p\big) = -(-1/_p) = -1,$$

which completes the argument. □

Next, we turn to the diagonalization of the Jacobsthal matrix. It is in this direction that we run into quadratic Gauss sums.

As a general fact, all circulant matrices of order n are diagonalized (over $\mathbb{C}$) by one and the same matrix–the Fourier matrix F_n. Recall, this is the invertible $n \times n$ matrix $F_n = (\zeta_n^{ab})_{0 \leq a,b \leq n-1}$. It is not hard to see that, conversely, a matrix which is diagonalized by the Fourier matrix F_n is a circulant matrix.

Lemma 1.16. *Let*

$$W = \begin{pmatrix} w_0 & w_{n-1} & \dots & w_1 \\ w_1 & w_0 & \dots & w_2 \\ & \dots & & \\ w_{n-1} & w_{n-2} & \dots & w_0 \end{pmatrix}$$

be a circulant matrix of order n, with complex entries. Then W is diagonalized by the Fourier matrix F_n; specifically, $F_n^{-1} W F_n$ is the diagonal matrix

$$\mathrm{diag}\left(\sum_{k=0}^{n-1} w_k \, \zeta_n^{-kb} : b = 0, \dots, n-1\right).$$

Proof. Let D denote the diagonal matrix described above. We aim to check that $WF_n = F_n D$. We view the entries of the circulant matrix W as being given by the formula $W_{ab} = w_{a-b}$ for $0 \leq a, b \leq n-1$, where the index is interpreted modulo n. Then

$$\begin{aligned} (WF_n)_{ab} &= \sum_{c=0}^{n-1} W_{ac} \, (F_n)_{cb} = \sum_{c=0}^{n-1} w_{a-c} \, \zeta_n^{cb} = \zeta_n^{ab} \sum_{c=0}^{n-1} w_{a-c} \, \zeta_n^{-(a-c)b} \\ &= \zeta_n^{ab} \sum_{k=0}^{n-1} w_k \, \zeta_n^{-kb} = (F_n)_{ab} \, D_{bb} = (F_n D)_{ab}. \end{aligned}$$

We have thereby verified $WF_n = F_n D$ entry by entry. □

Returning to the diagonalization of the Jacobsthal matrix, we obtain the following.

Theorem 1.17. *The Jacobsthal matrix Q_p is diagonalized by the Fourier matrix F_p; specifically,*

$$F_p^{-1} Q_p F_p = \begin{cases} \mathrm{diag}\big((b/_p)\sqrt{p} : b = 0, \dots, p-1\big) & \textit{if } p \equiv 1 \textit{ mod } 4, \\ \mathrm{diag}\big(-i(b/_p)\sqrt{p} : b = 0, \dots, p-1\big) & \textit{if } p \equiv 3 \textit{ mod } 4. \end{cases}$$

Proof. By the previous lemma, $F_p^{-1}Q_pF_p$ is the diagonal matrix whose entries are

$$\sum_{k=0}^{p-1} (k/_p)\, \zeta_p^{-kb}$$

for $b = 0, \dots, p-1$. As we have already seen in the proof of Lemma 1.11, the above sum equals $(-b/_p)\,\Gamma_p$ whenever $b \neq 0$. This continues to hold for $b = 0$, since both sides vanish in this case. Thus

$$F_p^{-1}Q_pF_p = \mathrm{diag}\big((-b/_p)\,\Gamma_p : b = 0, \dots, p-1\big).$$

This can be made very explicit, by using the evaluation of the quadratic Gauss sum Γ_p. If $p \equiv 1 \bmod 4$, we have $\Gamma_p = \sqrt{p}$; furthermore, $(-1/_p) = 1$. In this case we obtain $F_p^{-1}Q_pF_p = \mathrm{diag}\big((b/_p)\sqrt{p} : b = 0, \dots, p-1\big)$. If $p \equiv 3 \bmod 4$, we have $\Gamma_p = i\sqrt{p}$ and $(-1/_p) = -1$. We then have $F_p^{-1}Q_pF_p = \mathrm{diag}\big(-i(b/_p)\sqrt{p} : b = 0, \dots, p-1\big)$. □

The eigenvalues of the Jacobsthal matrix Q_p are listed along the diagonals, as if on a clothesline, ready to be read off:

- when $p \equiv 1 \bmod 4$, the eigenvalues of Q_p are 0, with multiplicity one, and $\pm\sqrt{p}$, each with multiplicity $(p-1)/2$;
- when $p \equiv 3 \bmod 4$, the eigenvalues of Q_p are 0, with multiplicity one, and $\pm i\sqrt{p}$, each with multiplicity $(p-1)/2$.

If the eigenvalues of Q_p is all that we are after, there is a quicker way to get them. Indeed, they can be gleaned from the relation $Q_p^2 = (-1/_p)\,(pI_p - J_p)$. The matrix J_p has two eigenvalues, 0 and p, the latter being simple; therefore the matrix $pI_p - J_p$ has eigenvalues p and 0, the latter being simple. We infer that Q_p has 0 as a simple eigenvalue, and the remaining $p-1$ eigenvalues satisfy $\lambda^2 = (-1/_p)\,p$. When $p \equiv 1 \bmod 4$, we have $(-1/_p) = 1$ and so $\lambda = \pm\sqrt{p}$. When $p \equiv 3 \bmod 4$, we have $(-1/_p) = -1$ and so $\lambda = \pm i\sqrt{p}$. Since the eigenvalues sum up to the trace of Q_p, which is 0, we deduce that, in each case, the two possible signs occur equally often.

Application 1.18. A *Hadamard matrix* of order n is an n-by-n matrix whose entries are 1 or -1, and whose rows are mutually orthogonal. For example,

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is a Hadamard matrix of order 2. When $n \geq 3$, a simple combinatorial argument shows that a necessary condition for the existence of a Hadamard matrix of order n is that $n \equiv 0 \bmod 4$. A long-standing open question asks the converse: does there exist a Hadamard matrix of order n, for every $n \equiv 0 \bmod 4$?

Here are two constructions of Hadamard matrices that have the Jacobsthal matrix at their core:

if p is a prime and $p \equiv 3 \bmod 4$, then

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Q_p - I_p & \\ 1 & & & \end{pmatrix}$$

is a Hadamard matrix of order $p+1$;

if p is a prime and $p \equiv 1 \bmod 4$, set

$$M_{\pm} = \begin{pmatrix} \pm 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Q_p \pm I_p & \\ 1 & & & \end{pmatrix};$$

then

$$\begin{pmatrix} M_+ & M_- \\ M_- & -M_+ \end{pmatrix}$$

is a Hadamard matrix of order $2(p+1)$.

We leave it as an exercise for the reader to check that the matrices are indeed Hadamard, as claimed. Suffices to say that the argument exploits the properties of Q_p that we have already listed. Firstly, $Q_p \pm I_p$ has all its entries 1 or -1. Secondly, Q_p is symmetric and $Q_p^2 = pI_p - J_p$ when $p \equiv 1 \bmod 4$, respectively Q_p is antisymmetric and $Q_p^2 = -(pI_p - J_p)$ when $p \equiv 3 \bmod 4$.

Notes. The remarkable construction of Hadamard matrices, outlined above, is due to Paley [14].

2. Gauss sums over $\mathbb{F}_p$

> *Marco Polo describes a bridge, stone by stone. "But which is the stone that supports the bridge?" Kublai Khan asks. "The bridge is not supported by one stone or another," Marco answers, "but by the line of the arch that they form." Kublai Khan remains silent, reflecting. Then he adds: "Why do you speak of the stones? It is only the arch that matters to me." Polo answers: "Without stones there is no arch."* (Italo Calvino, *Invisible Cities*)

2.1. **Characters of finite abelian groups.** Let G be a finite abelian group. The operation of G is written multiplicatively, and its identity element is denoted by 1. The cardinality of G is denoted $|G|$.

A *character* χ of G is a group homomorphism $\chi : G \to \mathbb{C}^*$. That is to say, χ is a complex-valued map on G satisfying $\chi(gh) = \chi(g)\chi(h)$ for all $g, h \in G$. Note that $\chi(1) = 1$, though one should bear in mind that the two 1's are different, in general.

Lemma 2.1. *Let χ be a character of G. Then*

(i) $|\chi(g)| = 1$ for all $g \in G$;
(ii) $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.

Proof. (i) Put $n = |G|$. Then each $g \in G$ satisfies $g^n = 1$ and so $\chi(g)^n = \chi(g^n) = \chi(1) = 1$ in $\mathbb{C}^*$, whence $|\chi(g)| = 1$. In fact, not only does χ take values in the unit circle, its values are actually among the n-th roots of unity. Next,

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

which proves (ii). □

Let $\widehat{G}$ denote the set of characters of G. Then $\widehat{G}$ is a group under pointwise multiplication, the neutral element being the trivial character $\mathbb{1}$ given by $\mathbb{1}(g) = 1$ for all $g \in G$. The inverse, in $\widehat{G}$, of a character χ is $\chi^{-1} = \overline{\chi}$. The finite abelian group $\widehat{G}$ is called the *dual* of G.

Here is a key example.

Example 2.2. Consider the additive group $\mathbb{Z}/n\mathbb{Z}$. A character χ is determined by the value $\chi(1)$, where $1 \in \mathbb{Z}/n\mathbb{Z}$ is the canonical generator. As $\chi(1)$ is an n-th root of unity in $\mathbb{C}$, we have $\chi(1) = \zeta_n^k$ for a unique $k \in \{0, \dots, n-1\}$. The corresponding character is given by

$$\chi_k(a) = \zeta_n^{ak}.$$

So the dual group of $\mathbb{Z}/n\mathbb{Z}$ is $\widehat{\mathbb{Z}/n\mathbb{Z}} = \{\chi_k : k = 0, \dots, n-1\}$. This is a cyclic group with n elements, generated by the character χ_1. The map $k \mapsto \chi_k$ defines a group isomorphism $\mathbb{Z}/n\mathbb{Z} \longrightarrow \widehat{\mathbb{Z}/n\mathbb{Z}}$.

A key upshot of the above example is that $\widehat{G}$ is isomorphic to G, whenever G is a finite cyclic group. Now every finite abelian group is isomorphic to a direct product of finite cyclic groups, and taking duals is compatible with direct products–in the sense that $\widehat{G_1 \times G_2}$ is naturally isomorphic to $\widehat{G_1} \times \widehat{G_2}$ for any two finite abelian groups G_1 and G_2. The verification of this latter fact is left to the reader. We thus reach the following conclusion.

Theorem 2.3. *Let G be a finite abelian group. Then the dual $\widehat{G}$ is isomorphic to G. In particular, G has exactly $|G|$ characters.*

The previous theorem is one of the core facts in the character theory for finite abelian groups. The next two are concerned with certain fundamental character sums, and they are sometimes referred to as the orthogonality relations. It will be convenient to start using the *Iverson bracket* notation: if P is a statement, then

$$\llbracket P \rrbracket = \begin{cases} 1 & \text{if } P \text{ is true,} \\ 0 & \text{if } P \text{ is false.} \end{cases}$$

Theorem 2.4. *For each character χ of G we have*

$$\sum_{g \in G} \chi(g) = |G| \llbracket \chi = \mathbb{1} \rrbracket = \begin{cases} 0 & \text{if } \chi \neq \mathbb{1}, \\ |G| & \text{if } \chi = \mathbb{1}. \end{cases}$$

Proof. When $\chi = \mathbb{1}$, we clearly have $\sum_{g \in G} \chi(g) = 1$. The interesting part is proving that $\sum_{g \in G} \chi(g) = 0$ whenever $\chi \neq \mathbb{1}$. Indeed, for each $h \in G$ we have

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g).$$

As χ is non-trivial, there exists $h \in G$ with $\chi(h) \neq 1$. The desired vanishing follows. □

Theorem 2.5. *For each element $g \in G$ we have*

$$\sum_{\chi \in \widehat{G}} \chi(g) = |G| [\![g = 1]\!] = \begin{cases} 0 & \textit{if } g \neq 1, \\ |G| & \textit{if } g = 1. \end{cases}$$

Proof. We calculate

$$\begin{aligned} \sum_{g \in G} \Big| \sum_{\chi \in \widehat{G}} \chi(g) \Big|^2 &= \sum_{g \in G} \Big(\sum_{\chi_1 \in \widehat{G}} \chi_1(g) \Big) \Big(\sum_{\chi_2 \in \widehat{G}} \overline{\chi_2}(g) \Big) \\ &= \sum_{\chi_1, \chi_2 \in \widehat{G}} \sum_{g \in G} (\chi_1 \overline{\chi_2})(g). \end{aligned}$$

By the previous theorem, the inner sum equals $|G| [\![\chi_1 \overline{\chi_2} = \mathbb{1}]\!] = |G| [\![\chi_1 = \chi_2]\!]$ and so we can continue as follows:

$$\sum_{g \in G} \Big| \sum_{\chi \in \widehat{G}} \chi(g) \Big|^2 = |G| \sum_{\chi_1, \chi_2 \in \widehat{G}} [\![\chi_1 = \chi_2]\!] = |G| |\widehat{G}| = |G|^2.$$

The term corresponding to $g = 1$ is $\sum_{\chi \in \widehat{G}} \chi(1) = |\widehat{G}| = |G|$. We deduce from the above formula that $\sum_{\chi \in \widehat{G}} \chi(g) = 0$ whenever $g \neq 1$. □

We note that, over the group $\mathbb{Z}/n\mathbb{Z}$, the previous theorem yields (1).

The finite-dimensional space of complex-valued functions on G can be endowed with the natural scalar product

$$\langle \alpha, \beta \rangle = \sum_{g \in G} \alpha(g) \, \overline{\beta(g)}.$$

Viewed in this light, Theorem 2.4 implies that $\langle \chi, \mathbb{1} \rangle = 0$ for each non-trivial character χ–that is to say, χ is orthogonal to the trivial character $\mathbb{1}$. Actually, more is true: distinct characters are orthogonal. We have brushed past this fact in the proof of Theorem 2.5. If $\chi_1 \neq \chi_2$ then

$$\langle \chi_1, \chi_2 \rangle = \sum_{g \in G} \chi_1(g) \, \overline{\chi_2(g)} = \sum_{g \in G} (\chi_1 \overline{\chi_2})(g) = 0$$

since the character $\chi_1 \overline{\chi_2}$ is non-trivial.

There are $|G|$ characters of G, as many as the dimension of the space of complex-valued functions on G, and they form an orthogonal set. So the following holds.

Theorem 2.6. *The characters of G form an orthogonal basis for the space of complex-valued functions on G.*

2.2. **Incomplete character sum estimates: the square-root bound.** Let G be a finite abelian group. A sum of the form

$$\sum_{g\in A} \chi(g),$$

where χ is a character of G, and A is a subset of G, is known as an *incomplete character sum*. In applications, such a sum counts an arithmetic occurrence (encoded by χ) within a restricted range (the subset A). The explicit evaluation of an incomplete character sum is an exceptionally rare event. Instead, one usually aims for estimates on its magnitude.

The trivial bound, which follows from the fact that $|\chi(g)| = 1$ for each $g \in G$, is

$$\Big|\sum_{g\in A} \chi(g)\Big| \leq |A|.$$

This uniform bound is attained by the trivial character $\chi = \mathbb{1}$, so let us focus on non-trivial characters. We will show that the *square-root bound*

$$\Big|\sum_{g\in A} \chi(g)\Big| \leq \sqrt{|A|}$$

holds on average. This can actually be interpreted in two different ways–that we vary χ while keeping A fixed, or that we vary A, subject to a fixed size, while keeping χ fixed. It is a comforting fact that both ways lead to the same outcome.

Theorem 2.7. *Let $A \subseteq G$ be non-empty, and let χ be a non-trivial character of G. Then*

$$\mathbb{E}\Big|\sum_{g\in A} \chi(g)\Big| \leq \sqrt{|A|}$$

in two ways:

- *for each A, as χ runs over the non-trivial characters of G;*
- *for each χ, as A runs over the subsets of G of a given size.*

We recall that the expected value of a random variable $f : \Omega \to \mathbb{R}$, defined over a finite sample space Ω, is

$$\mathbb{E}f = \frac{1}{|\Omega|}\sum_{\omega\in\Omega} f(\omega).$$

In general, we have $(\mathbb{E}|f|)^2 \leq \mathbb{E}(|f|^2)$ by a simple application of the Cauchy-Schwarz inequality. The expected value of $|f|^2$ turns out to be easier to compute in a number of situations that exhibit 'orthogonality', such as the character context we are in.

Lemma 2.8. *Let $A \subseteq G$ be non-empty, and let χ be a non-trivial character of G. Then*

$$\mathbb{E}\Big|\sum_{g\in A} \chi(g)\Big|^2 = \frac{|A||A^c|}{|G|-1}$$

in two ways:

- *for each A, as χ runs over the non-trivial characters of G;*
- *for each χ, as A runs over the subsets of G of a given size.*

We remark that the symmetry $A \leftrightarrow A^c$ in the above outcome should not be a surprise. For if χ is a non-trivial character, then $\sum_{g\in A^c}\chi(g) = -\sum_{g\in A}\chi(g)$ and so $\big|\sum_{g\in A^c}\chi(g)\big| = \big|\sum_{g\in A}\chi(g)\big|$.

Theorem 2.7 is an immediate consequence of the lemma.

Proof. To begin with, we write

$$\Big|\sum_{g\in A}\chi(g)\Big|^2 = \Big(\sum_{g\in A}\chi(g)\Big)\Big(\sum_{h\in A}\overline{\chi(h)}\Big) = \sum_{g,h\in A}\chi(gh^{-1}).$$

Let $A \subseteq G$ be fixed non-empty subset. As χ runs over the non-trivial characters of G, we have

$$\begin{aligned}\mathbb{E}\Big|\sum_{g\in A}\chi(g)\Big|^2 &= \frac{1}{|G|-1}\sum_{\chi\neq\mathbb{1}}\Big|\sum_{g\in A}\chi(g)\Big|^2\\ &= \frac{1}{|G|-1}\sum_{g,h\in A}\sum_{\chi\neq\mathbb{1}}\chi(gh^{-1}).\end{aligned}$$

By Theorem 2.5, the inner sum is $|G|[\![gh^{-1}=1]\!]-1 = |G|[\![g=h]\!]-1$. Hence

$$\begin{aligned}\mathbb{E}\Big|\sum_{g\in A}\chi(g)\Big|^2 &= \frac{1}{|G|-1}\sum_{g,h\in A}\big(|G|[\![g=h]\!]-1\big)\\ &= \frac{|G||A|-|A|^2}{|G|-1} = \frac{|A||A^c|}{|G|-1}.\end{aligned}$$

Now let χ be a fixed non-trivial character of G. As A runs over the subsets of G of given size α, we have

$$\begin{aligned}\mathbb{E}\Big|\sum_{g\in A}\chi(g)\Big|^2 &= \binom{|G|}{\alpha}^{-1}\sum_{|A|=\alpha}\Big|\sum_{g\in A}\chi(g)\Big|^2\\ &= \binom{|G|}{\alpha}^{-1}\sum_{|A|=\alpha}\sum_{g,h\in A}\chi(gh^{-1}).\end{aligned}$$

The double sum can be written as

$$\sum_{g,h\in G}\chi(gh^{-1})\cdot\big|\{A\subseteq G : g,h\in A, |A|=\alpha\}\big|$$

and the latter count is $\binom{|G|-1}{\alpha-1}$ when $g=h$, respectively $\binom{|G|-2}{\alpha-2}$ when $g\neq h$. So the above double sum evaluates as

$$\binom{|G|-1}{\alpha-1}\sum_{g\in G}\chi(1)+\binom{|G|-2}{\alpha-2}\sum_{g\neq h}\chi(gh^{-1}).$$

Here $\sum_{g\in G}\chi(1)=|G|$, and

$$\begin{aligned}\sum_{g\neq h}\chi(gh^{-1}) &= \sum_{g=h}\chi(gh^{-1}) - \sum_{g,h\in G}\chi(gh^{-1})\\ &= \sum_{g\in G}\chi(1) - \Big|\sum_{g\in G}\chi(g)\Big|^2 = |G|\end{aligned}$$

as well. We conclude that

$$\mathbb{E}\Big|\sum_{g\in A}\chi(g)\Big|^2 = \binom{|G|}{\alpha}^{-1}|G|\binom{|G|-2}{\alpha-1} = \frac{\alpha(|G|-\alpha)}{|G|-1}$$

as claimed. □

2.3. **Multiplicative characters of $\mathbb{F}_p$.**

Let $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements, where p is an odd prime. Two abelian group structures coexist on $\mathbb{F}_p$: the additive group $(\mathbb{F}_p,+)$, and the multiplicative group $(\mathbb{F}_p^*,\cdot)$; both are cyclic. A significant difference arises, however, when it comes to the cyclic generators. There is an explicit and canonical additive generator, namely 1, but a multiplicative generator is quite mysterious in general–neither explicit, nor canonical. In fact, finding one is a challenging problem from the computational viewpoint–no efficient algorithm is known for doing so.

Two types of characters can be associated to $\mathbb{F}_p$: *additive characters*, which are maps $\psi:\mathbb{F}_p\to\mathbb{C}^*$ satisfying $\psi(a)\psi(b)=\psi(a+b)$, respectively *multiplicative characters*, which are maps $\chi:\mathbb{F}_p^*\to\mathbb{C}^*$ satisfying $\chi(a)\chi(b)=\chi(ab)$. The additive characters can be described explicitly, as in Example 2.2, thanks to the canonical additive generator 1. The lack of a canonical multiplicative generator makes multiplicative characters more obscure. They are the main characters in what follows.

It is convenient to extend each multiplicative character χ, from $\mathbb{F}_p^*$ to the whole of $\mathbb{F}_p$. We do so by setting $\chi(0)=0$ when $\chi\neq\mathbb{1}$, respectively $\chi(0)=1$ when $\chi=\mathbb{1}$. Thus extended, a multiplicative character χ satisfies $\chi(a)\chi(b)=\chi(ab)$ for all $a,b\in\mathbb{F}_p$, and

$$\sum_{a\in\mathbb{F}_p}\chi(a)=p\llbracket\chi=\mathbb{1}\rrbracket=\begin{cases}0 & \text{if } \chi\neq\mathbb{1},\\ p & \text{if } \chi=\mathbb{1}.\end{cases}$$

Example 2.9. The Legendre symbol on $\mathbb{Z}$ descends to a multiplicative character of $\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$, denoted by σ and referred to as *the quadratic character* in what follows. Thus

$$\sigma(a)=({}^{a}/_{p})$$

for $a\in\{0,1,\ldots,p-1\}$. Note that the quadratic character is ±1 valued on $\mathbb{F}_p^*$, and already extended to $\mathbb{F}_p$ by $\sigma(0)=0$. The quadratic character has order 2; in fact, since the dual of the multiplicative group $\mathbb{F}_p^*$ is cyclic, it is the unique multiplicative character of order 2.

We recall that

$$\sigma(-1) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Lemma 2.10. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_p$, and let $a, b \in \mathbb{F}_p$. Then*

$$\sum_{c\in\mathbb{F}_p} \chi(c+a)\,\overline{\chi}(c+b) = p[\![a=b]\!] - 1 = \begin{cases} -1 & \text{if } a \neq b, \\ p-1 & \text{if } a = b. \end{cases}$$

Proof. We write

$$\sum_{c\in\mathbb{F}_p} \chi(c+a)\,\overline{\chi}(c+b) = \sum_{c\neq -b} \chi\Big(\frac{c+a}{c+b}\Big).$$

When $a = b$, the right-hand sum equals $(p-1)\chi(1) = p-1$. When $a \neq b$, we observe that $c \mapsto (c+a)/(c+b)$ is a bijection from $\mathbb{F}_p \setminus \{-b\}$ to $\mathbb{F}_p \setminus \{1\}$. Therefore the right-hand sum equals $-\chi(1) = -1$. □

For $\chi = \sigma$, the quadratic character, we recover Lemma 1.15 and its proof.

2.4. **Gauss sums.** The *Gauss sum* associated to a multiplicative character χ of $\mathbb{F}_p$ is

$$G(\chi) = \sum_{a\in\mathbb{F}_p} \chi(a)\,\zeta_p^a,$$

where, as usual, $\zeta_p = e^{2\pi i/p}$ is the 'first' p-th root of unity.

When χ is the trivial character, we have $G(\mathbb{1}) = \sum_{a\in\mathbb{F}_p} \zeta_p^a = 0$.

When χ is the quadratic character σ, Lemma 1.9 can be stated as saying that $G(\sigma) = \Gamma_p$, the quadratic Gauss sum of order p. We therefore have the following fact.

Theorem 2.11. *The Gauss sum corresponding to the quadratic character can be evaluated as*

$$G(\sigma) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \textit{ mod } 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \textit{ mod } 4. \end{cases}$$

As for Gauss sum associated to general non-trivial characters, we quickly abandon any hope of evaluating them. What we can evaluate, quite easily in fact, is their absolute value. This will play a crucial role in what follows.

Theorem 2.12. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_p$. Then*

$$\big|G(\chi)\big| = \sqrt{p}. \tag{11}$$

One way to prove Theorem 2.12 is by means of the following result of independent interest.

Lemma 2.13. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_p$, and let $c \in \mathbb{F}_p$. Then*

$$\sum_{a\in\mathbb{F}_p} \chi(a)\,\zeta_p^{ac} = \overline{\chi}(c)\,G(\chi). \tag{12}$$

Proof. If $c = 0$, then both sides of (12) vanish. If $c \neq 0$, then the change of variable $a \mapsto ac^{-1}$ yields

$$\sum_{a\in\mathbb{F}_p} \chi(a)\,\zeta_p^{ac} = \sum_{a\in\mathbb{F}_p} \chi(ac^{-1})\,\zeta_p^{a} = \chi(c^{-1}) \sum_{a\in\mathbb{F}_p} \chi(a)\,\zeta_p^{a} = \overline{\chi}(c)\,G(\chi),$$

and so (12) is verified in this case as well. □

Proof of Theorem 2.12. By (2), we have

$$\sum_{c\in\mathbb{F}_p} \Big| \sum_{a\in\mathbb{F}_p} \chi(a)\,\zeta_p^{ca} \Big|^2 = p \sum_{c\in\mathbb{F}_p} |\chi(c)|^2.$$

On the left-hand side, the inner-most sum equals $\overline{\chi}(c)\,G(\chi)$, thanks to (12). Thus, the above identity becomes

$$|G(\chi)|^2 \sum_{c\in\mathbb{F}_p} |\overline{\chi}(c)|^2 = p \sum_{c\in\mathbb{F}_p} |\chi(c)|^2.$$

The two sums are clearly identical, and non-vanishing; in fact, their value is $p-1$. It follows that $|G(\chi)|^2 = p$, whence the formula (11). □

The first remark concerning the identity (12) is that, by applying it for $c = -1$, we have

$$\overline{G(\chi)} = \sum_{a\in\mathbb{F}_p} \overline{\chi}(a)\,\zeta_p^{-a} = \chi(-1)\,G(\overline{\chi}). \tag{13}$$

Thus (11) can also be expressed as $G(\chi)\,G(\overline{\chi}) = \chi(-1)p$.

The second remark on (12) is that it can be put in the following form:

$$\overline{\chi}(a) = \frac{1}{G(\chi)} \sum_{c\in\mathbb{F}_p^*} \chi(c)\,\zeta_p^{ac}. \tag{14}$$

Note that we have dropped the index value $c = 0$, as $\chi(0) = 0$. The point of the above formula is that the left-hand side behaves multiplicatively in the argument a, whereas the right-hand side has an additive behavior. Subsequent results will illustrate the usefulness of this trade-off.

Notes. For the sake of conciseness we have restricted our attention to Gauss sums over $\mathbb{F}_p$. One may–and should– consider Gauss sums over a finite field, or over a modular ring $\mathbb{Z}/n\mathbb{Z}$. We refer the reader to Conrad's blurb [2] for a nice overview of these generalizations. The common case of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the simplest, yet arguably the most important–the main features of Gauss sums shine through, unburdened by technicalities.

2.5. **The Fourier matrix of order p, revisited.** Recall that the Fourier matrix of order p is given by $F_p = \big(\zeta_p^{rs}\big)_{0\leq r,s\leq p-1}$. We can presently make a key observation: that we can interpret (12) as saying that

$$F_p \cdot \chi = G(\chi)\,\overline{\chi} \tag{15}$$

for any non-trivial multiplicative character χ of $\mathbb{F}_p$. Here, we view χ as the column vector $(0 = \chi(0), 1 = \chi(1), \ldots, \chi(p-1)) \in \mathbb{C}^p$. Replacing χ by $\overline{\chi}$ yields

$$F_p \cdot \overline{\chi} = G(\overline{\chi})\,\chi. \tag{16}$$

Taken together, the relations (15) and (16) suggest that two linear combination of χ and $\overline{\chi}$ are eigenvectors of F_p. This is what the first part of the next theorem states, though casting out the quadratic character σ. In the case when $\chi = \sigma$, the relations (15) and (16) are duplicates since σ is real-valued, and we simply get that σ is an eigenvector of F_p. The second part of the next theorem records this case. The third part completes the picture by finding the contribution of the remaining multiplicative character–the trivial character $\mathbb{1}$.

Theorem 2.14 (Eigenvectors of F_p)**.**

(i) Let $\chi \neq \mathbb{1}, \sigma$ be a multiplicative character of $\mathbb{F}_p$. Put

$$\epsilon(\chi) = \begin{cases} 1 & \text{if } \chi(-1) = 1, \\ i & \text{if } \chi(-1) = -1 \end{cases}$$

so that $\epsilon(\chi)^2 = \chi(-1)$. Then $v_\pm(\chi) = \pm\epsilon(\chi)\sqrt{p}\,\chi + G(\chi)\,\overline{\chi}$ is an eigenvector of F_p with eigenvalue $\pm\epsilon(\chi)\sqrt{p}$.

(ii) The quadratic character σ is an eigenvector of F_p with eigenvalue $G(\sigma)$.

(iii) Put $\mathbb{1}_0 = (1, 0, \ldots, 0) \in \mathbb{C}^p$. Then $v_\pm(\mathbb{1}) = \pm\sqrt{p}\,\mathbb{1}_0 + \mathbb{1}$ is an eigenvector of F_p with eigenvalue $\pm\sqrt{p}$.

Proof. (i) Let us first spell out the simple fact that $\chi(-1) = \pm 1$ for each multiplicative character χ of $\mathbb{F}_p$; this is implicit in the definition of the signing ϵ. The assumption that $\chi \neq \mathbb{1}, \sigma$ guarantees that χ and $\overline{\chi}$ are distinct, whence linearly independent. Therefore the vectors $v_+(\chi)$ and $v_-(\chi)$ are non-zero, in fact linearly independent as well.

Using (15) and (16), we compute

$$\begin{aligned} F_p \cdot v_+(\chi) &= \epsilon(\chi)\sqrt{p}(F_p \cdot \chi) + G(\chi)(F_p \cdot \overline{\chi}) \\ &= \epsilon(\chi)\sqrt{p}(G(\chi)\,\overline{\chi}) + G(\chi)(G(\overline{\chi})\,\chi). \end{aligned}$$

As $G(\chi)\,G(\overline{\chi}) = \chi(-1)p = \epsilon(\chi)^2 p$, we obtain

$$F_p \cdot v_+(\chi) = \epsilon(\chi)\sqrt{p}\big(G(\chi)\,\overline{\chi} + \epsilon(\chi)\sqrt{p}\,\chi\big) = \epsilon(\chi)\sqrt{p} \cdot v_+(\chi).$$

That is, $v_+(\chi)$ is an eigenvector of F_p with eigenvalue $\epsilon(\chi)\sqrt{p}$. A similar calculation shows that $v_-(\chi)$ is an eigenvector of F_p with eigenvalue $-\epsilon(\chi)\sqrt{p}$.

(ii) This is (15), and (16) as well, in the case when $\chi = \sigma$.

(iii) We have

$$F_p \cdot \mathbb{1} = p\mathbb{1}_0, \qquad F_p \cdot \mathbb{1}_0 = \mathbb{1}.$$

The latter relation simply reflects the fact that the first row of F_p consists of 1's. The former relation, a bit more interesting, owes to (1). We then have

$$F_p \cdot v_+(\mathbb{1}) = \sqrt{p}\, F_p \cdot \mathbb{1}_0 + F_p \cdot \mathbb{1} = \sqrt{p}\, \mathbb{1} + p\mathbb{1}_0 = \sqrt{p}\, v_+(\mathbb{1}),$$

and similarly $F_p \cdot v_-(\mathbb{1}) = -\sqrt{p}\, v_-(\mathbb{1})$. Obviously, $v_+(\mathbb{1})$ and $v_-(\mathbb{1})$ are non-zero, so they are eigenvectors with corresponding eigenvalues $\sqrt{p}$ and $-\sqrt{p}$. □

Let us tally up the eigenvectors we have obtained in Theorem 2.14. The starting point is the basis for the complex-valued functions on $\mathbb{F}_p^*$, consisting of the $p-1$ multiplicative characters of $\mathbb{F}_p$. When extended to $\mathbb{F}_p$, the multiplicative characters remain independent; adding the function $\mathbb{1}_0$ yields a basis for the complex-valued functions on $\mathbb{F}_p$. The eigenvectors for the Fourier matrix F_p that we have obtained are localized perturbations of the multiplicative characters of $\mathbb{F}_p$.

The trivial character $\mathbb{1}$ contributes two eigenvectors, $v_+(\mathbb{1})$ and $v_-(\mathbb{1})$. The quadratic character cuts a solitary figure: it is the only multiplicative character of $\mathbb{F}_p$ that is an eigenvector for F_p. There are $(p-3)/2$ doublets of conjugate, non-real multiplicative characters $\{\chi, \overline{\chi}\}$; each such doublet contributes two eigenvectors, $v_+(\chi)$ and $v_-(\chi)$. The grand total is p distinct eigenvectors.

Theorem 2.15. *The p eigenvectors of F_p, as described in Theorem 2.14, form an orthogonal basis.*

Proof. We set aside for a moment the eigenvector of F_p given by the quadratic character. The remaining $p-1$ eigenvectors span the same 2-dimensional subspaces as their seed vectors. Namely, $v_+(\mathbb{1})$ and $v_-(\mathbb{1})$ span the same plane as $\mathbb{1}$ and $\mathbb{1}_0$, and for each doublet of conjugate, non-real multiplicative characters $\{\chi, \overline{\chi}\}$, the eigenvectors $v_+(\chi)$ and $v_-(\chi)$ span the same plane as χ and $\overline{\chi}$. Consequently, the p eigenvectors are spanning, and so they form a basis.

Let us consider the orthogonality aspect. To begin with, the characters of the multiplicative group $\mathbb{F}_p^*$ are orthogonal; they remain so upon extending them to $\mathbb{F}_p$. The function $\mathbb{1}_0$, which we add so as to obtain a basis, is orthogonal to the non-trivial multiplicative characters but not to the trivial character $\mathbb{1}$.

Much of this orthogonality is preserved when passing to the p eigenvectors of F_p. The only pairs whose orthogonality is in question are $v_+(\mathbb{1})$ and $v_-(\mathbb{1})$, respectively $v_+(\chi)$ and $v_-(\chi)$ for each non-real multiplicative character χ. We check these directly:

$$\begin{aligned}\langle v_+(\mathbb{1}), v_-(\mathbb{1})\rangle &= \langle \sqrt{p}\, \mathbb{1}_0 + \mathbb{1}, -\sqrt{p}\, \mathbb{1}_0 + \mathbb{1}\rangle\\ &= -p\langle \mathbb{1}_0, \mathbb{1}_0\rangle + \langle \mathbb{1}, \mathbb{1}\rangle = -p + p = 0,\end{aligned}$$

and

$$\begin{aligned}\langle v_+(\chi), v_-(\chi)\rangle &= \big\langle \epsilon(\chi)\sqrt{p}\, \chi + G(\chi)\, \overline{\chi}, -\epsilon(\chi)\sqrt{p}\, \chi + G(\chi)\, \overline{\chi}\big\rangle\\ &= -|\epsilon(\chi)|^2 p\langle \chi, \chi\rangle + |G(\chi)|^2\langle \overline{\chi}, \overline{\chi}\rangle\\ &= -p(p-1) + p(p-1) = 0.\end{aligned}$$

Of course, the orthogonality of the p eigenvectors also implies that they form a basis. □

Example 2.16. It is quite instructive to pick a small prime p and to work out, very explicitly, the eigen-picture of the Fourier matrix F_p that we have described above. The reasonable choice is $p = 5$.

We first tabulate the characters of the multiplicative group $\mathbb{F}_5^*$. They are determined by their value on a chosen generator, say 2. Besides the trivial character $\mathbb{1}$ and the quadratic character σ, there is one doublet $\{\chi, \overline{\chi}\}$ of conjugate, non-real multiplicative characters.

$\mathbb{F}_5^*$	$\mathbb{1}$	σ	χ	$\overline{\chi}$
2	1	-1	i	$-i$
4	1	1	-1	-1
3	1	-1	$-i$	i
1	1	1	1	1

Next, we extend the multiplicative characters to $\mathbb{F}_5$, and we add the function $\mathbb{1}_0$ so as to obtain a basis for the complex-valued functions on $\mathbb{F}_5$.

$\mathbb{F}_5$	$\mathbb{1}_0$	$\mathbb{1}$	σ	χ	$\overline{\chi}$
0	1	1	0	0	0
1	0	1	1	1	1
2	0	1	-1	i	$-i$
3	0	1	-1	$-i$	i
4	0	1	1	-1	-1

As $\chi(-1) = -1$, we have $\epsilon(\chi) = i$. So we can tabulate the eigenvectors of F_5 provided by Theorem 2.14 as follows.

$\mathbb{F}_5$	$v_+(\mathbb{1})$	$v_-(\mathbb{1})$	σ	$v_+(\chi)$	$v_-(\chi)$
0	$\sqrt{5}+1$	$-\sqrt{5}+1$	0	0	0
1	1	1	1	$i\sqrt{5}+G(\chi)$	$-i\sqrt{5}+G(\chi)$
2	1	1	-1	$-\sqrt{5}-iG(\chi)$	$\sqrt{5}-iG(\chi)$
3	1	1	-1	$\sqrt{5}+iG(\chi)$	$-\sqrt{5}+iG(\chi)$
4	1	1	1	$-i\sqrt{5}-G(\chi)$	$i\sqrt{5}-G(\chi)$

We evaluate the Gauss sum associated to the character χ:

$$\begin{aligned}
G(\chi) &= \chi(1)\,\zeta_5 + \chi(2)\,\zeta_5^2 + \chi(3)\,\zeta_5^3 + \chi(4)\,\zeta_5^4 \\
&= \zeta_5 + i\zeta_5^2 - i\zeta_5^3 - \zeta_5^4 = \zeta_5 - \overline{\zeta_5} + i\big(\zeta_5^2 - \overline{\zeta_5^2}\big) \\
&= 2i\sin\left(\frac{2\pi}{5}\right) - 2\sin\left(\frac{4\pi}{5}\right) \\
&= -\sqrt{\frac{5-\sqrt{5}}{2}} + i\sqrt{\frac{5+\sqrt{5}}{2}}.
\end{aligned}$$

In the last step, we used the elementary evaluations

$$\sin\left(\frac{2\pi}{5}\right)=\sqrt{\frac{5+\sqrt{5}}{8}},\qquad \sin\left(\frac{4\pi}{5}\right)=\sqrt{\frac{5-\sqrt{5}}{8}},$$

which are probably best derived from the simpler-looking evaluations

$$\cos\left(\frac{2\pi}{5}\right)=\frac{\sqrt{5}-1}{4},\qquad \cos\left(\frac{4\pi}{5}\right)=\frac{-\sqrt{5}-1}{4}.$$

Using the latter formulas, it is easy to evaluate the quadratic Gauss sum. The point is that we do so directly, without an appeal to Theorem 2.11.

$$\begin{aligned} G(\sigma) &= \sigma(1)\,\zeta_5+\sigma(2)\,\zeta_5^2+\sigma(3)\,\zeta_5^3+\sigma(4)\,\zeta_5^4\\ &= \zeta_5-\zeta_5^2-\zeta_5^3+\zeta_5^4=\zeta_5+\overline{\zeta_5}-\left(\zeta_5^2+\overline{\zeta_5^2}\right)\\ &= 2\cos\left(\frac{2\pi}{5}\right)-2\cos\left(\frac{4\pi}{5}\right)\\ &= \sqrt{5}. \end{aligned}$$

The eigenvalues of F_5 are $\pm\epsilon(\chi)\sqrt{5}=\pm i\sqrt{5}$, $G(\sigma)=\sqrt{5}$, and then $\pm\sqrt{5}$.

Another upshot of Theorem 2.14 is an alternate proof of Theorem 2.11. The point is that we can get an explicit list of all eigenvalues of F_p, other than $G(\sigma)$. Recall that our original pathway to Theorem 2.11 was through Theorem 1.4.

Alternate proof of Theorem 2.11. From Theorem 2.14 we read off the following eigenvalues of F_p: $\pm\epsilon(\chi)\sqrt{p}$, each one with multiplicity $(p-3)/2$, $\pm\sqrt{p}$, and $G(\sigma)$. This is a complete listing of the eigenvalues of F_p, since the corresponding eigenvectors form a basis. To get an explicit spectral picture, we need to understand the distribution of $\epsilon(\chi)$, as χ runs over the non-real multiplicative characters of $\mathbb{F}_p^*$. Let $n_\pm$ denote the number of doublets $\{\chi,\overline{\chi}\}$ of conjugate, non-real characters satisfying $\chi(-1)=\overline{\chi}(-1)=\pm1$. On the one hand,

$$n_+ + n_- = \frac{p-3}{2}.$$

On the other hand, the summation formula

$$\sum_{\chi\in\widehat{\mathbb{F}_p^*}}\chi(-1)=0$$

yields the relation $1+\sigma(-1)+2n_+-2n_-=0$. We obtain

$$n_+=\frac{p-\sigma(-1)-4}{4},\qquad n_-=\frac{p+\sigma(-1)-2}{4}.$$

In summary, the p eigenvalues of F_p are as follows: $\pm\sqrt{p}$, each with multiplicity $1+n_+$; $\pm i\sqrt{p}$, each with multiplicity n_-; and $G(\sigma)$. Our aim is to show that

$$G(\sigma)=\begin{cases}\sqrt{p} & \text{if } p\equiv 1 \bmod 4,\\ i\sqrt{p} & \text{if } p\equiv 3 \bmod 4.\end{cases}$$

To do so, we recall Lemma 1.6, which tells us that the determinant of F_p is a positive multiple of $(-i)^{(p-1)/2}$. Our present knowledge of the eigenvalues of F_p allows us to compute

$$\begin{aligned}\det F_p &= (\sqrt{p})^{1+n_+} \cdot (-\sqrt{p})^{1+n_+} \cdot (i\sqrt{p})^{n_-} \cdot (-i\sqrt{p})^{n_-} \cdot G(\sigma)\\ &= (-1)^{1+n_+ + n_-} \cdot i^{2n_-} \cdot p^{1+n_+ + n_-} \cdot G(\sigma)\\ &= (-1)^{(p-1)/2} \cdot i^{(p+\sigma(-1)-2)/2} \cdot p^{(p-1)/2} \cdot G(\sigma)\\ &= \begin{cases} i^{(p-1)/2} \cdot p^{(p-1)/2} \cdot G(\sigma) & \text{if } p \equiv 1 \bmod 4,\\ -i^{(p-3)/2} \cdot p^{(p-1)/2} \cdot G(\sigma) & \text{if } p \equiv 3 \bmod 4. \end{cases}\end{aligned}$$

We deduce that $G(\sigma)$ is positive when $p \equiv 1 \bmod 4$, respectively a positive multiple of i when $p \equiv 3 \bmod 4$. Since $|G(\sigma)| = \sqrt{p}$, thanks to (11), we conclude that $G(\sigma) = \sqrt{p}$ when $p \equiv 1 \bmod 4$, respectively $G(\sigma) = i\sqrt{p}$ when $p \equiv 3 \bmod 4$. □

As soon as the value of the quadratic Gauss sum is known, the eigenvalues of F_p–including their multiplicities–can be completely spelled out. We tabulate them below.

$p \equiv 1 \bmod 4$:

eigenvalue	$\sqrt{p}$	$-\sqrt{p}$	$i\sqrt{p}$	$-i\sqrt{p}$
multiplicity	$(p+3)/4$	$(p-1)/4$	$(p-1)/4$	$(p-1)/4$

$p \equiv 3 \bmod 4$:

eigenvalue	$\sqrt{p}$	$-\sqrt{p}$	$i\sqrt{p}$	$-i\sqrt{p}$
multiplicity	$(p+1)/4$	$(p+1)/4$	$(p+1)/4$	$(p-3)/4$

We have thereby obtained a different approach to the result of Theorem 1.4 in the prime order case.

Notes. The alternate approach to the evaluation of the quadratic Gauss sum adapts an argument due to Waterhouse [22]. It is worthwhile emphasizing that the following two problems go hand in hand, and may be even construed as being equivalent: (i) the determination of the eigenvalues (and their multiplicities) for the Fourier matrix F_p, and (ii) the evaluation of the quadratic Gauss sum $G(\sigma)$. Our first approach was to solve (i), and then deduce (ii). In this section, we saw how (i) hinges on (ii).

Eigenbases of the Fourier matrix of order n have received quite a bit of attention; see, for instance, [10, 13, 5, 7, 20, 11, 8]. There is a lot of freedom in building eigenbases since the four eigenspaces have high dimension. For a generalization of the character-based approach described herein, see Morton [13].

2.6. **Incomplete character sum estimates: double sums.** The following result is an additive analogue of Application 1.3.

Theorem 2.17. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_p$, and let $A, B \subseteq \mathbb{F}_p$. Then*

$$\Big|\sum_{a\in A}\sum_{b\in B}\chi(a+b)\Big| \leq \sqrt{p^{-1}|A||B||A^c||B^c|}.$$

We note that a simpler, but coarser, upper bound is $\sqrt{p|A||B|}$.

Somewhat surprisingly, the proof will make use of Gauss sums. Let us first describe a direct argument–not involving Gauss sums–that will yield a slightly weaker upper bound. This argument bears a strong resemblance to the approach taken in Application 1.3.

A weaker bound. We begin by estimating

$$\Big|\sum_{a\in A}\sum_{b\in B}\chi(a+b)\Big|^2 \leq |A|\sum_{a\in A}\Big|\sum_{b\in B}\chi(a+b)\Big|^2 \leq |A|\sum_{a\in\mathbb{F}_p}\Big|\sum_{b\in B}\chi(a+b)\Big|^2.$$

The first estimate is an application of the Cauchy-Schwarz inequality; in the second estimate, we complete the outer sum. The point now is that the latter, half-completed double sum can be evaluated as follows. We write

$$\begin{aligned}\sum_{a\in\mathbb{F}_p}\Big|\sum_{b\in B}\chi(a+b)\Big|^2 &= \sum_{a\in\mathbb{F}_p}\Big(\sum_{b\in B}\chi(a+b)\Big)\Big(\sum_{b'\in B}\overline{\chi(a+b')}\Big)\\ &= \sum_{b,b'\in B}\sum_{a\in\mathbb{F}_p}\chi(a+b)\overline{\chi}(a+b').\end{aligned}$$

Thanks to Lemma 2.10, we know that the inner sum equals $p[\![b=b']\!]-1$. Therefore

$$\sum_{b,b'\in B}\sum_{a\in\mathbb{F}_p}\chi(a+b)\overline{\chi}(a+b') = p\sum_{b,b'\in B}[\![b=b']\!] - \sum_{b,b'\in B}1 = p|B|-|B|^2.$$

Overall, we obtain the bound

$$\Big|\sum_{a\in A}\sum_{b\in B}\chi(a+b)\Big| \leq \sqrt{|A|\big(p|B|-|B|^2\big)} = \sqrt{|A||B|\big(p-|B|\big)}.$$

Note, however, that A and B play symmetric roles; so the upper bound can be improved to $\sqrt{|A||B|\big(p-\max\{|A|,|B|\}\big)}$. This is better than the simple upper bound $\sqrt{p|A||B|}$, but still weaker than the desired upper bound. □

As already mentioned, the better argument exploits Gauss sums.

Proof of Theorem 2.17. By (14), we have

$$\sum_{a\in A}\sum_{b\in B}\overline{\chi}(a+b) = \frac{1}{G(\chi)}\sum_{c\in\mathbb{F}_p^*}\chi(c)\sum_{a\in A}\sum_{b\in B}\zeta_p^{(a+b)c}.$$

We take absolute values; as χ is non-trivial, we have $|G(\chi)| = \sqrt{p}$, and we deduce that

$$\Big|\sum_{a\in A}\sum_{b\in B}\chi(a+b)\Big| \leq \frac{1}{\sqrt{p}}\sum_{c\in\mathbb{F}_p^*}\Big|\sum_{a\in A}\sum_{b\in B}\zeta_p^{(a+b)c}\Big|.$$

The next step is bounding the inner double sum over A and B. Here, we are aided by the fact that we can separate A from B. Indeed:

$$\sum_{a\in A}\sum_{b\in B}\zeta_p^{(a+b)c} = \Big(\sum_{a\in A}\zeta_p^{ac}\Big)\Big(\sum_{b\in B}\zeta_p^{bc}\Big),$$

whence

$$\begin{aligned}\sum_{c\in\mathbb{F}_p^*}\Big|\sum_{a\in A}\sum_{b\in B}\zeta_p^{(a+b)c}\Big| &= \sum_{c\in\mathbb{F}_p^*}\Big|\sum_{a\in A}\zeta_p^{ac}\Big|\Big|\sum_{b\in B}\zeta_p^{bc}\Big| \\ &\leq \Big(\sum_{c\in\mathbb{F}_p^*}\Big|\sum_{a\in A}\zeta_p^{ac}\Big|^2\Big)^{1/2}\Big(\sum_{c\in\mathbb{F}_p^*}\Big|\sum_{b\in B}\zeta_p^{bc}\Big|^2\Big)^{1/2}\end{aligned}$$

by the Cauchy-Schwarz inequality. Now

$$\sum_{c\in\mathbb{F}_p^*}\Big|\sum_{a\in A}\zeta_p^{ac}\Big|^2 = p|A| - |A|^2 = |A||A^c|$$

by applying (3); an analogous evaluation holds over B as well. Overall, we have

$$\Big|\sum_{a\in A}\sum_{b\in B}\chi(a+b)\Big| \leq \frac{1}{\sqrt{p}}\sqrt{|A||A^c||B||B^c|}$$

as desired. □

Application 2.18. Let $A \subseteq \mathbb{F}_p$ have the property that the difference between any two distinct elements of A is a square in $\mathbb{F}_p$. For example, $\{1,4,5\}$ is such a set for $p = 13$. We note that a necessary condition for the existence of such a set is that -1 is a square in $\mathbb{F}_p$, that is to say, $p \equiv 1 \bmod 4$.

We then have the following double sum involving the quadratic character:

$$\sum_{a,b\in A}\sigma(a-b) = \sum_{a\in A}(|A|-1) = |A|(|A|-1).$$

On the other, by applying Theorem 2.17 to the sets A and $-A$, we know that

$$\Big|\sum_{a,b\in A}\sigma(a-b)\Big| \leq \frac{1}{\sqrt{p}}|A|(p-|A|).$$

Combining the two facts, we deduce that $|A| \leq \sqrt{p}$.

Notes. Theorem 2.17 was first noted by Erdős and Shapiro [6], and then by Chung [1] in the stronger form stated herein.

The bound $|A| \leq \sqrt{p}$ from Application 2.18 is probably folklore, as there are many ways to obtain it. Can it be improved, possibly below the square-root bound? This is a well-known problem in additive combinatorics; see, e.g., Croot - Lev [3, Problem 2.8]. The best result known so far is the following modest improvement, recently proved by Hanson and Petridis [9]: $|A| \leq \sqrt{p/2}+1$. The conjectural expectation, however, is that for each $\epsilon > 0$ the bound $|A| \leq p^{\epsilon}$ should hold for large enough p.

2.7. Incomplete character sum estimates: the Pólya–Vinogradov inequality.

Let us say that a subset $A \subseteq \mathbb{F}_p$ is an *arc of length* m, where $m < p$, if it is of the form $A = \{t, t+1, \dots, t+m-1\}$.

Theorem 2.19. *Let χ be a non-trivial multiplicative character of $\mathbb{F}_p$. Then, for any arc $A \subseteq \mathbb{F}_p$, we have*

$$\Big|\sum_{a\in A} \chi(a)\Big| < \sqrt{p}\,\log p. \tag{17}$$

There are two points to be noticed about the upper bound in (17): firstly, it is very close to being on the order of $\sqrt{p}$; secondly, it is independent of the arc's length. In keeping with the usage in number theory, the logarithm in (17) is the natural logarithm with base e.

The proof of the bound (17) combines two ideas: that multiplicative characters can be expressed in terms of the additive ones, by means of the formula (14), and that the additive analogue of (17) can be handled rather easily by using the assumption that A is an arc. The argument will also need a delightful exercise in calculus!

Proof. By using (14), we can write

$$\sum_{a\in A} \overline{\chi}(a) = \frac{1}{G(\chi)} \sum_{b\in \mathbb{F}_p^*} \chi(b) \sum_{a\in A} \zeta_p^{ab}.$$

Taking absolute values, and keeping in mind that $|G(\chi)| = \sqrt{p}$, we deduce that

$$\Big|\sum_{a\in A} \chi(a)\Big| \leq \frac{1}{\sqrt{p}} \sum_{k=1}^{p-1} \Big|\sum_{a\in A} \zeta_p^{ak}\Big|.$$

Now we make use of the specific form of A. For each $k \in \{1, \dots, p-1\}$ we have:

$$\sum_{a\in A} \zeta_p^{ak} = \zeta_p^{tk} \sum_{j=0}^{m-1} \zeta_p^{jk} = \zeta_p^{tk} \cdot \frac{1-\zeta_p^{mk}}{1-\zeta_p^{k}}$$

since $\zeta_p^k \neq 1$. Therefore

$$\Big|\sum_{a\in A} \zeta_p^{ak}\Big| = \frac{|1-\zeta_p^{mk}|}{|1-\zeta_p^{k}|} \leq \frac{2}{|1-\zeta_p^{k}|} = \frac{1}{\sin(k\pi/p)}.$$

Summarizing, we have shown that

$$\Big|\sum_{a\in A} \chi(a)\Big| \leq \frac{1}{\sqrt{p}} \sum_{k=1}^{p-1} \frac{1}{\sin(k\pi/p)}.$$

We give an upper bound for the latter sum in a separate lemma, see below. The lemma's bound implies that

$$\Big|\sum_{a\in A}\chi(a)\Big| < \frac{2\sqrt{p}}{\pi}\,\log\frac{4p}{\pi}.$$

It is a simple matter to verify that this bound is in fact better than the desired bound (17), for any $p \geq 3$. □

Lemma 2.20. *We have*

$$\sum_{k=1}^{p-1}\frac{1}{\sin(k\pi/p)} < \frac{2p}{\pi}\,\log\frac{4p}{\pi}.$$

Proof. We start from the observation that the left-hand side resembles a Riemann sum for the function $f(x) = \sin(\pi x)^{-1}$. Which brings us to the following general fact: if f is a convex, continuous function on the interval $(0, 1)$, then

$$\frac{1}{p}\sum_{k=1}^{p-1} f\left(\frac{k}{p}\right) \leq \int_{1/(2p)}^{1-1/(2p)} f(x)\,dx.$$

This can be seen by interpreting the left-hand side as the midpoint Riemann sum over the partition $1/(2p) < 3/(2p) < \cdots < (2p-1)/(2p)$. Convexity implies that such a midpoint Riemann sum underestimates the Riemann integral. Thus, denoting $\epsilon = 1/(2p)$, we obtain

$$\begin{aligned}\frac{1}{p}\sum_{k=1}^{p-1}\frac{1}{\sin(k\pi/p)} &\leq \int_{\epsilon}^{1-\epsilon}\frac{1}{\sin(\pi x)}\,dx \\ &= \frac{1}{\pi}\int_{\pi\epsilon}^{\pi(1-\epsilon)}\csc x\,dx = \frac{2}{\pi}\int_{\pi\epsilon}^{\pi/2}\csc x\,dx\end{aligned}$$

by a change of variable, and a use of symmetry. We now work out the definite integral. Recall that $\log|\csc x - \cot x|$ is an antiderivative of $\csc(x)$; we write

$$\csc x - \cot x = \frac{1-\cos x}{\sin x} = \frac{2\sin^2(x/2)}{2\sin(x/2)\cos(x/2)} = \tan(x/2).$$

We then get

$$\int_{\pi\epsilon}^{\pi/2}\csc(x)\,dx = \log\big|\tan(x/2)\big|\,\Big|_{\pi\epsilon}^{\pi/2} = \log\frac{1}{\tan(\pi\epsilon/2)}.$$

Next, we use the inequality $\tan x > x$, valid for any $x \in (0, \pi/2)$. We deduce that

$$\int_{\pi\epsilon}^{\pi/2}\csc(x)\,dx < \log\frac{1}{\pi\epsilon/2} = \log\frac{4p}{\pi}.$$

The claimed bound follows. □

Application 2.21. Just like Application 2.18, the most immediate use of the Pólya–Vinogradov inequality pertains to the quadratic character:

$$\Big|\sum_{a\in A}\sigma(a)\Big| < \sqrt{p}\ \log p$$

for any arc $A\subseteq\mathbb{F}_p$.

If we assume that each element of the arc A is a non-square, then we obtain $|A|<\sqrt{p}\ \log p$. We interpret this as a fact about the spacing of squares: any two consecutive squares in $\mathbb{F}_p=\{0,1,\ldots,p-1\}$ are at most $\sqrt{p}\ \log p$ apart.

A similar argument, this time assuming the arc A to consist of squares only, shows that the same spacing bound holds for non-squares as well.

The next result puts the Pólya–Vinogradov inequality (17) into perspective. It shows, in particular, that the main term in the upper bound, $\sqrt{p}$, is unavoidable.

Theorem 2.22. *Given $m\in\{1,\ldots,p-1\}$, there exist positive constants c_m, C_m so that the following holds: for each non-trivial multiplicative character χ of $\mathbb{F}_p$, we have*

$$c_m\sqrt{p}\leq \mathbb{E}\Big|\sum_{a\in A}\chi(a)\Big|\leq C_m\sqrt{p}$$

as A runs over the arcs of length m.

Proof. Put $\delta=m/p$. There are p arcs of length $m=\delta p$, namely $A(t)=\{t,t+1,\ldots,t+m-1\}$ for each $t\in\mathbb{F}_p$. The desired expected value is

$$\mathbb{E}\Big|\sum_{a\in A}\chi(a)\Big|=\frac{1}{p}\sum_{t\in\mathbb{F}_p}\Big|\sum_{a\in A(t)}\chi(a)\Big|.$$

The upper bound. This part bears some resemblance with Lemma 2.8. The main ingredient here is the fact that, for any subset $A\subseteq\mathbb{F}_p$, we have

$$\sum_{t\in\mathbb{F}_p}\Big|\sum_{a\in t+A}\chi(a)\Big|^2=|A||A^c|.$$

Indeed, we can expand

$$\Big|\sum_{a\in t+A}\chi(a)\Big|^2=\Big|\sum_{a\in A}\chi(t+a)\Big|^2=\sum_{a,b\in A}\chi(t+a)\overline{\chi}(t+b).$$

Using Lemma 2.10 along the way, we compute

$$\begin{aligned}\sum_{t\in\mathbb{F}_p}\Big|\sum_{a\in t+A}\chi(a)\Big|^2&=\sum_{a,b\in A}\ \sum_{t\in\mathbb{F}_p}\chi(t+a)\overline{\chi}(t+b)\\&=\sum_{a,b\in A}\big(p[\![a=b]\!]-1\big)=p|A|-|A|^2=|A||A^c|.\end{aligned}$$

In the case at hand, we take $A=A(0)$, and so $t+A=A(t)$. We deduce that

$$\mathbb{E}\Big|\sum_{a\in A}\chi(a)\Big|^2=\frac{|A(0)||A(0)^c|}{p}=\delta(1-\delta)p.$$

Using the inequality $(\mathbb{E}|f|)^2 \leq \mathbb{E}|f|^2$, it follows that

$$\mathbb{E}\Big|\sum_{a\in A}\chi(a)\Big| \leq \sqrt{\delta(1-\delta)}\,\sqrt{p} = C_m\sqrt{p}.$$

The lower bound. This part of the argument uses Gauss sums. Put

$$S = \sum_{t\in\mathbb{F}_p}\Big(\sum_{a\in A(t)}\chi(a)\Big)\zeta_p^t.$$

On the one hand,

$$|S| \leq \sum_{t\in\mathbb{F}_p}\Big|\sum_{a\in A(t)}\chi(a)\Big|$$

and so

$$\frac{|S|}{p} \leq \mathbb{E}\Big|\sum_{a\in A}\chi(a)\Big|.$$

On the other hand, S admits a simple closed form. Indeed, we can write

$$S = \sum_{t\in\mathbb{F}_p}\sum_{a\in A(0)}\chi(t+a)\zeta_p^t = \sum_{a\in A(0)}\sum_{t\in\mathbb{F}_p}\chi(t+a)\zeta_p^t.$$

The change of variable $t := t-a$ reveals that the inner sum equals $G(\chi)\zeta_p^{-a}$. Therefore

$$S = \sum_{a\in A(0)} G(\chi)\zeta_p^{-a} = G(\chi)\sum_{j=0}^{m-1}\zeta_p^{-j} = G(\chi)\cdot\frac{1-\zeta_p^{-m}}{1-\zeta_p^{-1}}.$$

Taking absolute values, we deduce that

$$|S| = \sqrt{p}\cdot\frac{|1-\zeta_p^m|}{|1-\zeta_p|} = \sqrt{p}\cdot\frac{\sin(m\pi/p)}{\sin(\pi/p)}.$$

We expect the latter fraction to have a lower estimate on the order of m. We note that $\sin x < x$ for $x > 0$, and $\sin x > 2x/\pi$ for $0 < x \leq \pi/2$; the latter bound can be checked by showing that $(\sin x)/x$ is decreasing on $(0,\pi/2]$. A combined use of these bounds confirms our expectation:

$$\frac{\sin(m\pi/p)}{\sin(\pi/p)} > \frac{2m/p}{\pi/p} = \frac{2m}{\pi}.$$

In summary, we have shown that

$$|S| > \frac{2m\sqrt{p}}{\pi} = \frac{2\delta}{\pi}p\sqrt{p}$$

and so

$$\mathbb{E}\Big|\sum_{a\in A}\chi(a)\Big| \geq \frac{|S|}{p} > \frac{2\delta}{\pi}\sqrt{p} = c_m\sqrt{p}.$$

This completes the proof. □

Notes. Theorem 2.19 is due, independently, to Pólya [16] and Vinogradov [21]. The proof presented herein is due to Schur [17]. Schur also proved what, in our account, is the lower bound in Theorem 2.22.

References

[1] Fan R.K. Chung: *Several generalizations of Weil sums*, J. Number Theory 49 (1994), no.1, 95–106

[2] Keith Conrad: *Gauss and Jacobi sums on finite fields and* $\mathbb{Z}/m\mathbb{Z}$, expository note available at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/Gauss-Jacobi-sums.pdf`

[3] Ernest S. Croot, Vsevolod F. Lev: *Open problems in additive combinatorics*, in 'Additive Combinatorics', CRM Proc. Lecture Notes no.43, 207–233, American Mathematical Society 2007

[4] William D'Alessandro: *Proving quadratic reciprocity: explanation, disagreement, transparency and depth*, Synthese 198 (2021), no.9, 8621–8664

[5] Bradley W. Dickinson, Kenneth Steiglitz: *Eigenvectors and functions of the discrete Fourier transform*, IEEE Trans. Acoust. Speech Signal Process. 30 (1982), no.1, 25–31

[6] Paul Erdős, Harold N. Shapiro: *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861–865

[7] F. Alberto Grünbaum: *The eigenvectors of the discrete Fourier transform: a version of the Hermite functions*, J. Math. Anal. Appl. 88 (1982), no.2, 355–363

[8] Shamgar Gurevich, Ronny Hadani: *On the diagonalization of the discrete Fourier transform*, Appl. Comput. Harmon. Anal. 27 (2009), no.1, 87–99

[9] Brandon Hanson, Giorgis Petridis: *Refined estimates concerning sumsets contained in the roots of unity*, Proc. Lond. Math. Soc. (3) 122 (2021), no.3, 353–358

[10] James H. McClellan, Thomas W. Parks: *Eigenvalue and eigenvector decomposition of the discrete Fourier transform*, IEEE Trans. Audio Electroacoust. 20 (1972), no.1, 66–74

[11] Madan Lal Mehta: *Eigenvalues and eigenvectors of the finite Fourier transform*, J. Math. Phys. 28 (1987), no. 4, 781–785

[12] Victor H. Moll: *An elementary trigonometric equation*, Coll. Math. J. 39 (2008), 395–398

[13] Patrick Morton: *On the eigenvectors of Schur's matrix*, J. Number Theory 12 (1980), no.1, 122–127

[14] Raymond E.A.C. Paley: *On orthogonal matrices*, J. Math. Phys. 12 (1933), 311–320

[15] Samuel J. Patterson: *Gauss sums*, in 'The Shaping of Arithmetic after C.F. Gauss's *Disquisitiones Arithmeticae*', edited by C. Goldstein, N. Schappacher, and J. Schwermer, 505–527, Springer 2007

[16] George Pólya: *Über die Verteilung der quadratischen Reste und Nichtreste*, Gött. Nachr. (1918), 21–29

[17] Issai Schur: *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya*, Gött. Nachr. (1918), 30–36

[18] Issai Schur: *Über die Gaussschen Summen*, Gött. Nachr. (1921), 147–153

[19] Balasubramanian Sury: *Nothing lucky about* 13, Math. Mag. 83 (2010), no. 4, 289–293

[20] Richard Tolimieri: *The construction of orthonormal bases diagonalizing the discrete Fourier transform*, Adv. in Appl. Math. 5 (1984), no.1, 56–86

[21] Ivan M. Vinogradov: *Über die Verteilung der quadratischen Reste und Nichtreste*, J. Soc. Phys. Math. Univ. Permi 2 (1919), 1–14

[22] William C. Waterhouse: *The sign of the Gaussian sum*, J. Number Theory 2 (1970), 363

Department of Mathematical Sciences
Indiana University Indianapolis
Email address: `bnica@iu.edu`