258

2. Georg Cantor, Über unendliche lineare Punktmannigfaltigkeiten, Nr.6, *Math. Annalen* **23** (1884) 453–488. doi:10.1007/BF01446598
3. Georg Cantor, Über eine elemtare Frage de Mannigfaltigketslehre, *Jahresberich der Deutsch. Math. Vereing. Bd. I*, S. 75–78 (1890–1891).
4. Joseph Dauben, *Georg Cantor: His Mathematics and Philosophy of the Infinite*, Princeton University Press, Princeton, NJ, 1990.
5. Richard Dedekind, *Essays on the Theory of Numbers. I: Continuity and Irrational Numbers; II: The Nature and Meaning of Numbers*, authorized translation by Wooster Woodruff Beman, Dover, New York, 1963.
6. Hal Hellman, *Great Feuds in Mathematics: Ten of the Liveliest Disputes Ever*, John Wiley, Hoboken, NJ, 2006.
7. Manya Janaky Raman, *Understanding Compactness: A Historical Perspective*, M.A. thesis, University of California Berkeley, 1997.
8. Jacqueline Stedall, *Mathematics Emerging: A Sourcebook 1540–1900,* Oxford University Press, New York, 2008.

Summary This expository note describes some of the history behind Georg Cantor's proof that the real numbers are uncountable. In fact, Cantor gave three different proofs of this important but initially controversial result. The first was published in 1874 and the famous diagonalization argument was not published until nearly two decades later. We explore the different ideas used in each of his three proofs.

Nothing Lucky about 13

B. SURY
Stat-Math Unit, Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560 059 India
sury@isibang.ac.in

Recently, a high school teacher came across the following problem which he passed on to a forum for mathematics teachers:

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

One could solve this in a number of elementary ways, and as we will show below, the value turns out to be $\frac{-1+\sqrt{13}}{4}$. The point here is to find what is special about 13 and about 2, 6, 8.

Without further ado, let us break the illusion that 13 might be particularly "lucky" to admit such a simple expression: We show a corresponding result for every prime number congruent to 1 modulo 4 and, indeed, for every prime.

Here we will explain briefly how to prove for any prime number $p \equiv 1$ modulo 4 the identity

$$\sum_{a \in Q} \cos\left(\frac{2a\pi}{p}\right) = \frac{-1+\sqrt{p}}{2}, \tag{1}$$

where the sum is over the set Q of quadratic residues mod p; that is, $a \in Q$ if $1 \leq a \leq p-1$ and for some integer b, $a \equiv b^2 \bmod p$. When $p \equiv 1 \bmod 4$, then -1 is a square mod p; indeed, for those who know it, we mention that Wilson's congruence $(p-1)! \equiv -1 \bmod p$ simplifies to $((\frac{p-1}{2})!)^2 \equiv -1 \bmod p$ in the case $p \equiv 1 \bmod 4$. Thus the squares mod p (as well as the nonsquares mod p) come in pairs $a, -a$ with

Math. Mag. **83** (2010) 289–293. doi:10.4169/002557010X521840.

exactly one of these less than or equal to $(p-1)/2$. As $\cos(t) = \cos(-t)$, the identity (1) could be rewritten as

$$\sum_{\substack{a \in Q \\ a \le (p-1)/2}} \cos\left(\frac{2a\pi}{p}\right) = \frac{-1+\sqrt{p}}{4},$$

and this explains the opening result, as the squares mod 13 are $\pm 1, \pm 3, \pm 4$.

The identity mentioned for primes congruent to 1 mod 4 has an analog for primes congruent to -1 mod 4.

The secret is the so-called Gauss sum, which Gauss used to prove the quadratic reciprocity law. Let p be an odd prime. The Gauss sum is the expression $\sum_{a=1}^{p-1} \pm z^a$, with $z = e^{2i\pi/p}$, where we use a plus sign if a is a square mod p and put a minus sign if a is not. The Legendre symbol $\left(\frac{a}{p}\right)$, which denotes 1 or -1 depending on whether a is a square mod p or not, allows us to express this more clearly: Write

$$G := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) z^a.$$

It is a remarkable fact that $G^2 = \pm p$ with the sign determined by whether $p \equiv \pm 1$ mod 4. With some care for the signs, we can show that G is $\sqrt{p}$ or $i\sqrt{p}$ as p is 1 or -1 mod 4 [**1**, pp. 70–76]. We have, therefore,

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) z^a = \begin{cases} \sqrt{p} & \text{if } p \equiv +1 \bmod p, \text{ and} \\ i\sqrt{p} & \text{if } p \equiv -1 \bmod p. \end{cases} \tag{2}$$

(A different choice of primitive pth root of unity as z can lead to a different sign for G.)

In this note we will first show how to use (2) to prove identities like (1) and its analogy for primes congruent to -1 mod 4. After this main result, we make a brief tour of the history of Gauss sums and, specifically, of the determination of their signs. Finally, we give a proof of (2).

The main result is :

THEOREM. *Let p be an odd prime and let Q be the subset of squares in $\mathbb{Z}_p^*$. Then,*

(i) *if $p \equiv 1$ mod 4, so that $Q = T \cup -T$ with $T \subseteq \{1, \ldots, \frac{p-1}{2}\}$, then*

$$\sum_{a \in Q} \cos\left(\frac{2a\pi}{p}\right) = 2\sum_{b \in T} \cos\left(\frac{2b\pi}{p}\right) = \frac{-1+\sqrt{p}}{2}.$$

(ii) *If $p \equiv -1$ mod 4, so that $\mathbb{Z}_p^* = Q \cup -Q$, then*

$$\sum_{a \in Q} \sin\left(\frac{2a\pi}{p}\right) = \frac{\sqrt{p}}{2} \quad \text{and} \quad \sum_{a \in Q} \cos\left(\frac{2a\pi}{p}\right) = \frac{-1}{2}.$$

Remark The prime 2 is special and, when we apply the proof below to it, we get the trivial identity $\cos(\pi) = -1$.

Proving the theorem We consider first the case when $p \equiv 1$ mod 4, when $Q = T \cup -T$ with $T \subseteq \{1, \ldots, \frac{p-1}{2}\}$. If N denotes the nonsquares mod p,

$$G = \sqrt{p} = \sum_{a \in Q} z^a - \sum_{b \in N} z^b.$$

On the other hand, since it is well known that the sum of the roots of unity sum to zero, we have

$$-1 = \sum_{c \in \mathbb{Z}_p^*} z^c = \sum_{a \in Q} z^a + \sum_{b \in N} z^b. \tag{3}$$

Adding the two equations and substituting $z = e^{2ip/p}$, we have

$$-1 + \sqrt{p} = 2 \sum_{a \in Q} z^a = \sum_{a \in Q} (z^a + z^{-a}) = \sum_{a \in Q} 2 \cos\left(\frac{2a\pi}{p}\right)$$

which is our first claim.

If $p \equiv -1 \bmod 4$, so that $\mathbb{Z}_p^* = Q \cup -Q$, then $G = i\sqrt{p}$ gives

$$\sum_{a \in Q} (z^a - z^{-a}) = i\sqrt{p};$$

which quickly simplifies to $\sum_{a \in Q} 2 \sin(2a\pi/p) = \sqrt{p}$. The second identity in (ii) follows immediately from (3).

Some history of Gauss sums Gauss sums were introduced by Gauss in 1801, when he stated some of their properties and used them to prove the quadratic reciprocity law in different ways. Gauss wrote that he had studied since 1805 the theory of cubic and biquadratic residues and, since results for these proved elusive, that he was motivated to find more proofs of the quadratic reciprocity law, hoping that one of them would yield a generalization for higher reciprocity laws. Gauss's fourth and sixth proofs of the quadratic reciprocity law used Gauss sums and, indeed, proved successful in investigating higher reciprocity laws.

The sign of the Gauss sum was a notoriously difficult question; he recorded the correct assertion in his mathematical diary in May 1801, but could find a proof only in 1805. He says in a letter to Olbers written in September 1805 that he was annoyed by this inability to determine the sign and that hardly a week went by for those 4 years when he did not make one or more unsuccessful attempt. He says that finally the mystery was solved "the way lightning strikes" [**1**].

As mentioned earlier, if z is a primitive pth root of unity, the sign of the sum $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) z^a$ depends on the choice of z. However, the key observation seems to be that the equality

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) z^a = \prod_{b=1}^{(p-1)/2} (z^{-b/2} - z^{b/2})$$

holds for any choice of primitive pth root of unity z. This can be deduced from a result on polynomials and, it is in this context that Gauss introduced the so-called Gaussian polynomials which generalize the binomial coefficients. Proofs to determine the sign of the Gauss sum were found later by Kronecker, Schur, Mertens, etc. A beautiful proof by Schur appears in Landau's classic German text [**2**, pp. 162–166]. Although Ireland and Rosen is a convenient modern reference for the Gauss sum computation [**1**, pp. 70–76], we take the liberty of recalling Schur's proof briefly for the sake of English-speaking readers.

THEOREM. *Let $n > 0$ be odd. Then $S := \sum_{s=0}^{n-1} e^{2i\pi s^2/n} = \sqrt{n}$ or $i\sqrt{n}$ depending on whether $n \equiv \pm 1$ mod 4.*

Before proving this result, we mention that when n is prime, $S = G$, the Gauss sum. This is again due to the observation that $\sum_{a=0}^{p-1} e^{2i\pi a/p} = 0$ mentioned earlier.

Proof (Schur). Put $z = e^{2i\pi/n}$ and consider the $n \times n$ matrix $A = (z^{kl})_{0\le k,l<n}$. Our sum is $S = \sum_k z^{k^2} = \operatorname{tr} A = \sum_{r=1}^{n} \lambda_r$, where $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of A. Viewing S as the trace of a matrix involving roots of unity proves advantageous because sums involving roots of unity often admit lots of cancellations.

The u, v entry of A^2 is $(A^2)_{u,v} = \sum_w z^{(u+v)w} = b_{u+v}$, where $b_m = \sum_w z^{mw}$. If $n \mid m$, then evidently $b_m = \sum_w z^{mw} = \sum_w 1 = n$. On the other hand, if $n \nmid m$, we have $z^m b_m = \sum_w z^{m(w+1)} = b_m$, which gives $b_m = 0$ since $z^m \ne 1$. Note that $\sum_r \lambda_r^2 = \operatorname{tr} A^2 = \sum_u b_{2u} = n$. Also, $(A^4)_{uv} = \sum_w b_{u+w} b_{w+v} = n^2$ or 0, depending on whether $u = v$ or not. Thus $A^4 = n^2 I$ where I is the $n \times n$ identity matrix.

The characteristic polynomial $\chi_{A^4}(\lambda)$ of A^4 is $(\lambda - n^2)^n$, which means that the eigenvalues $\lambda_1^4, \ldots, \lambda_n^4$ are all equal to n^2. In particular, $\lambda_r = i^{a_r}\sqrt{n}$ where $a_r = 0$, 1, 2, or 3. For each $k = 0, 1, 2, 3$, we count the number of eigenvalues with that power of i, by setting $m_k = |\{a_r : a_r = k\}|$. Note that $m_0 + m_1 + m_2 + m_3 = n$, because there are n eigenvalues.

We first show that $|S|^2 = n$. We start with

$$|S|^2 = S\bar{S} = \sum_{s=0}^{n-1} z^{s^2} \sum_{t=0}^{n-1} z^{-t^2} = \sum_{s,t} z^{s^2-t^2} = \sum_{s,t} z^{(s+t)^2-t^2}$$

$$= \sum_{s,t} z^{s^2+2st} = \sum_{s} \left(z^{s^2} \sum_{t} z^{2st} \right).$$

As $z = e^{2i\pi/n}$, we have $\sum_t z^{2st} = \sum_t e^{4i\pi st/n} = n$ or 0 depending on whether $n \mid s$ or not. Therefore, $|S|^2 = n$ and it remains to establish which square root gives the correct value of S.

Since S is determined in terms of the eigenvalues λ_rs which, in turn, depend on the m_is, we try to obtain linear equations satisfied by the m_is as a consequence of the equality $|S|^2 = n$. Continuing with the proof, since

$$S = \sum_r \lambda_r = \sum_r i^{a_r}\sqrt{n} = \sqrt{n}(m_0 + im_1 - m_2 - im_3)$$

and $|S|^2 = n$, we have $(m_0 - m_2)^2 + (m_1 - m_3)^2 = 1$. In other words, either $m_0 - m_2 = \pm 1$ and $m_1 = m_3$ or $m_0 = m_2$ and $m_1 - m_3 = \pm 1$. Hence $S = v\eta\sqrt{n}$ where $v = \pm 1$ and $\eta = 1$ or i. Thus, we have in terms of the m_is, the equation

$$m_0 + im_1 - m_2 - im_3 = v\eta$$

and its conjugate

$$m_0 - im_1 - m_2 + im_3 = v\eta^{-1}.$$

Also, the equality $\operatorname{tr} A^2 = \sum_r \lambda_r^2 = n$ observed earlier gives the equation

$$m_0 - m_1 + m_2 - m_3 = 1.$$

Thus, the system of four linear equations can be written as a matrix equation $Bx = y$, where

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \quad x = \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \end{pmatrix}, \quad \text{and} \quad y = \begin{pmatrix} n \\ v\eta \\ 1 \\ v\eta^{-1} \end{pmatrix}.$$

Inverting this matrix, we get $x = B^{-1}y$ with

$$B^{-1} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

In particular, $m_2 = \frac{n+1-v(\eta+\eta^{-1})}{4}$ being an integer implies that $\eta = 1$ or i, depending on whether $n \equiv 1 \bmod 4$ or $n \equiv 3 \bmod 4$. Further, $\det A = \prod_r \lambda_r = n^{n/2} i^{m_1+2m_2-m_3}$ $= n^{n/2} i^{3(n-1)/2} v = n^{n/2} i^{n(n-1)/2} v$; to obtain this, we have used the fact, obtained from $x = B^{-1}y$, that $m_1 + 2m_2 - m_3$ is $\frac{n+1}{2} - v$ or $\frac{n+1}{2} + v$ depending on whether $n \equiv 1$ or $3 \bmod 4$. We have also used $i^v = iv$ to simplify.

Finally, we show that $v = 1$: This will be a consequence of evaluating—in two different ways—the determinant of the matrix A:

$$\det A = \prod_{0 \le l < k < n} \left(e^{2i\pi k/n} - e^{2i\pi l/n}\right) = \prod_{l<k} e^{i\pi(k+l)/n}\left(e^{i\pi(k-l)/n} - e^{i\pi(l-k)/n}\right).$$

From $\sum_{0 \le l < k < n}(k+l) = n(n-1)^2/2$, we have

$$\prod_{l<k} e^{i\pi(k+l)/n} = e^{i\pi(n-1)^2/2} = i^{(n-1)^2} = 1.$$

Hence

$$\det A = \prod_{l<k}(e^{i\pi(k-l)/n} - e^{i\pi(l-k)/n}) = \prod_{l<k}\left(2i \sin\frac{\pi(k-l)}{n}\right)$$

$$= i^{n(n-1)/2} \prod_{l<k}\left(2 \sin\frac{\pi(k-l)}{n}\right).$$

As the last mentioned product is positive, the two expressions $\det A = n^{n/2} i^{n(n-1)/2} v = i^{n(n-1)/2} \prod_{l<k}\left(2 \sin\frac{\pi(k-l)}{n}\right)$ imply that $v > 0$ and is, therefore, equal to 1. ∎

Acknowledgment Initially, I was tempted to discuss a bit of the fascinating history surrounding Gauss sums but avoided it as this note was a short one. However, one of the referees raised this matter and mentioned that this is a "missed opportunity." This encouraged and emboldened me to add historical as well as mathematical material, which perhaps gives a better understanding of the background. It is a great pleasure to acknowledge the constructive comments from both the referees.

REFERENCES

1. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.
2. E. Landau, *Vorlesungen Uber Zahlentheorie aus der elementaren zahlentheorie*, Chelsea Publishing, New York, 1950.

Summary Gauss sums were introduced by Gauss in 1801, when he stated some of their properties and used them to prove the quadratic reciprocity law in different ways. The determination of the sign of the Gauss sum was a notoriously difficult question; Gauss recorded the correct assertion in his mathematical diary in May 1801, but could find a proof only in 1805. This note uses the Gauss sums to evaluate certain sums of trigonometric functions.