BMC Gauss Sums I 221102

Paul Zeitz, zeitzp@usfca.edu

This is an introduction to an amazing subject, *Gauss sums*, which merge number theory and algebra in surprising ways. It is a big subject, a good window into analytic number theory.

In the problems below we will explore a few properties of these sums, with the goal of proving one of Gauss's favorite achievements, the Law of Quadratic Reciprocity (LoQR). We assume that you—as an advanced BMC student—have seen LoQR before. But if not, Section 1 provides a quick summary.

Teaser problem

The following was by far the hardest problem on a local math contest that I organized some time ago. It inspires the topic of Gauss sums.

Let $\theta = 2\pi/17$. Compute the value of $\cos\theta + \cos 4\theta + \cos 9\theta + \cdots + \cos 16^2\theta$.

1 What is LoQR?

- A number a is called a *quadratic residue* modulo n if it is a "square" mod n; i.e., if there exists x such that $x^2 \equiv a \pmod{n}$. We will use the abbreviation QR for quadratic residue.
- Let p be a prime. If $a \perp p$ (i.e., a and p are relatively prime), define the *Legendre symbol* $\left(\frac{a}{p}\right)$ to equal 1 if a is a QR and -1 if a is not a QR $\pmod{p}$. Thus, for example, $\left(\frac{2}{7}\right) = 1$, since $3^2 \equiv 2 \pmod 7$, but $\left(\frac{3}{7}\right) = -1$, because there are no x satisfying $x^2 \equiv 3 \pmod 7$.
- We compute $(p-1)/2$ so frequently that we will denote it by h_p, where h means "half." If the prime is understood in context, we will just write h.

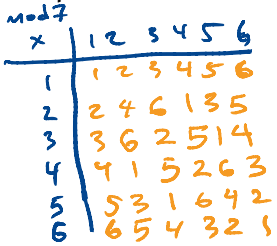
Statement of LoQR

Let p, q be two distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{h_p h_q} = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

2 Foundational stuff

In order to use Gauss sums (defined in Section 3), we need to make sure we can do some basic number theory and polynomial algebra. Assume that p is an odd prime and that $a \perp p$.



Exercise 1 ***The Sudoku priniciple.*** *Then the sets*

$$\{a, 2a, 3a, \ldots, (p-1)a\} \quad \text{and} \quad \{1, 2, 3, \ldots p-1\}$$

are equal $\pmod p$.

Exercise 2 *The equation* $x^2 \equiv a \pmod p$ *either has no solutions or exactly 2 solutions; consequently there are* h_p *QRs among the residues* $\{1, 2, 3, \ldots p-1\}$.

$3 \cdot 2 \equiv 3 \cdot 5 \mod 7$
$3 \cdot 2 - 3 \cdot 5 \equiv 0$
$3(2-5) \equiv 0$

Exercise 3 ***Wilson's theorem.*** *Prove that* $(p-1)! \equiv -1 \pmod p$.

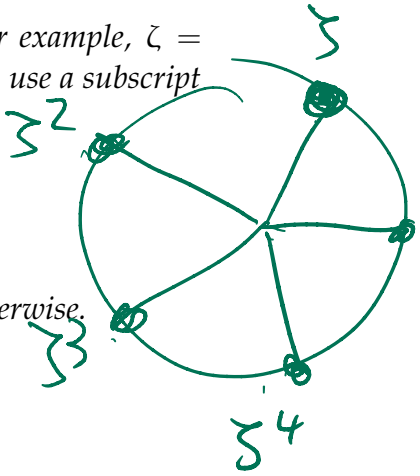
Exercise 4 ***Euler's criterion.*** *You proved Wilson's theorem by pairing, if able, terms in the product* $1 \cdot 2 \cdot 3 \cdots (p-1)$ *whose product was 1. Modify this so that the product is* **a** *to conclude that*

$$\left(\frac{a}{p}\right) \equiv a^h \pmod p.$$

Exercise 5 ***Roots of unity.*** *Let* ζ *be a primitive* p*th root of unity; for example,* $\zeta = \cos(2\pi/p) + i\sin(2\pi/p)$. *If we need to keep track of the prime* p*, we will use a subscript and write* ζ_p. *Prove the following:*

HW

1. $(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}) = 1 + x + x^2 + \cdots + x^{p-1}$.
2. $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$.
3. $1 + \zeta^k + \zeta^{2k} + \cdots = \zeta^{(p-1)k} = 0$ *as long as* $k \perp p$, *and equals* p *otherwise.*



3 Gauss sums

$\zeta^2, \zeta^4, \zeta^3, \zeta, 1$

The standard way to prove LoQR, done in most number theory classes, uses a sequence of lemmas: Euler's criterion, Gauss's lemma, Eisenstein's lemma, and then a clever lattice-point counting argument. It's great stuff. But we will take a different, more sophisticated route, using only Euler's criterion (Exercise 4), plus the new Gauss sum tools that we develop.

Fix an odd prime q. Define $e(t) = e^{2\pi i t} = \cos(2\pi t) + \sin(2\pi t)$. For an integer n, define the *Gauss sum*

$$G(n) = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) e(mn/q) = \sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \zeta^{mn},$$

where $\zeta = e(1/q)$ is a primitive qth root of unity.

HW: 5, 6, 7

Exercise 6 *Prove that* $G(n) = \left(\frac{n}{q}\right) G(1)$.

We will abbreviate $G = G(1)$, and use a subscript if we need to keep track of the prime. In other words, $G = G(1) = G_p$.

Let R, N denote nonzero quadratic residues or nonresidues, respectively. For example, if $q = 7$, then we have the sloppy but useful notation

$$\sum z^R = z + z^2 + z^4 \quad \text{and} \quad \sum z^N = z^3 + z^5 + z^6.$$

Exercise 7 *Let* $\zeta = e(1/q)$. *Show that* $\sum \zeta^R + \sum \zeta^N = -1$.

Exercise 8 *Show that*

$$G_q = \sum_{k=0}^{q-1} e(k^2/q).$$

(Notice that the index starts at zero.) Consequently, the sum in the Teaser Problem is equal to G_{17}.

The big question, of course, is what is G_q? Even Gauss found this difficult, and for our purposes, we will just compute the square of this quantity.

Exercise 9 *Show that*

$$G_p^2 = \begin{cases} p & \text{if } p \equiv 1 \pmod 4 \\ -p & \text{if } p \equiv 3 \pmod 4; \end{cases}$$

in other words,

$$G_p^2 = p\left(\frac{-1}{p}\right) \equiv p(-1)^h \pmod p.$$

$q = 17$

$\zeta = e^{2\pi i/17} = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$

$$G(n) := \sum_{a=1}^{16} \left(\frac{a}{17}\right)\zeta^{an}$$

$$G(1) = \sum_{a=1}^{16} \left(\frac{a}{17}\right)\zeta^{a}$$

Euler's Formula

$$\cos\theta + i\sin\theta = e^{i\theta}$$

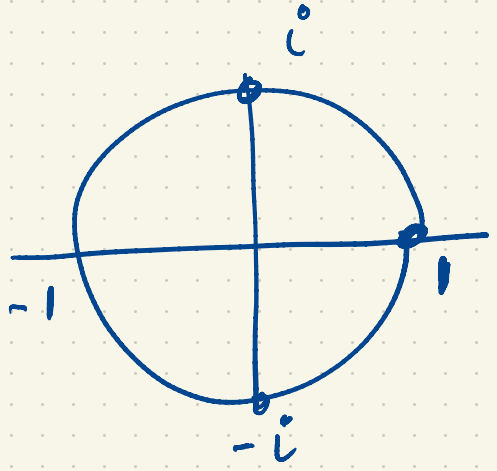
$$e^{i\theta}\, e^{i\beta} = e^{i(\theta+\beta)} =$$

$$e^{2\pi i\theta} = e(\theta)$$

$e(\frac{1}{17})$ = prim 17^{th} ROU.

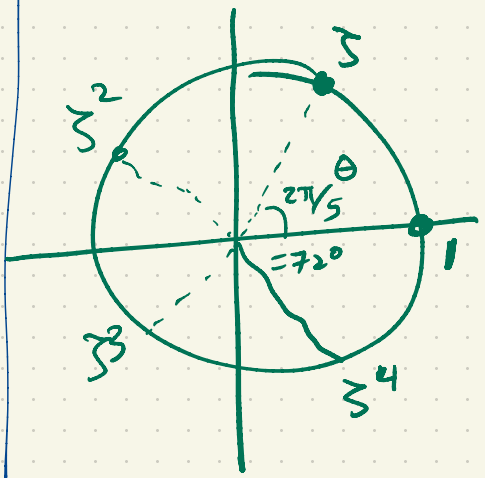
$x^4 = 1$

$x = 1, -1, i, -i$



$x^5 = 1$

$z^5 = 1$



$\zeta = \cos\theta + i\sin\theta$

$\theta = 72^\circ = 2\pi/5$

$z = \cos\theta + i\sin\theta$

$w = \cos\beta + i\sin\beta$

$zw = \cos(\theta+\beta) + i\sin(\theta+\beta)$

If $\theta = \frac{2\pi}{n}$ and $\zeta = \cos\theta + i\sin\theta$

Then $1, \zeta, \zeta^2, \zeta^3, \ldots \zeta^{n-1}$ are the n roots of $x^n = 1$

$p = 13$

$h = 6$

$a \equiv -1$

$a^h = (-1)^6 = 1 \pmod{13}$

-1 is a QR mod 13

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

$a = 2$

$2^6 = 64 \equiv -1 \bmod 13$

$\left(\frac{2}{13}\right) = -1$

$a = 3$ $\quad 3^6 = (3^3)^2 = 27^2 \equiv 1$

$\left(\frac{3}{13}\right) = 1$

Rule : x marrys y s.t. $xy \equiv 2$

Wilson $\Rightarrow$ $12! \equiv -1 \pmod{13}$

$= (12 \cdot 11) \cdot (10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3)(2 \cdot 1) \pmod{13}$

$$2^6 \equiv -1 \pmod{13}$$

---

new rule : x marrys y s.t. $xy = 3$ $\quad 4^2 \equiv 3$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \overset{13}{\equiv} -1$

$3^5 \cdot (4)(-4) \equiv -1 \quad = \quad -3^5 4^2 \equiv -3^5 \cdot 3 = -3^6 \equiv -1$

$3^6 \equiv +1$

$$a^h \equiv \left(\frac{a}{p}\right) \pmod{p}$$

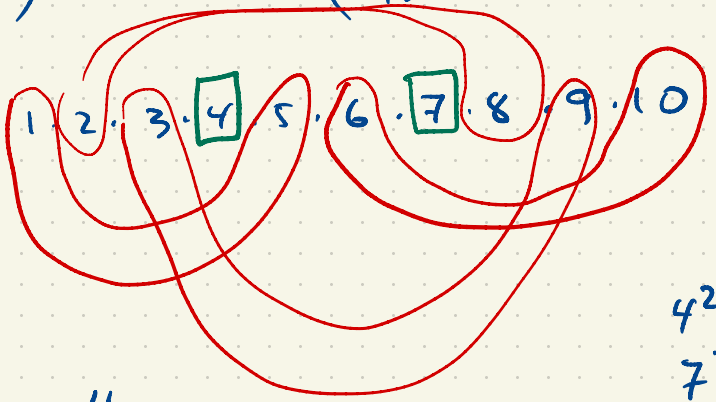
$p = 101$ $\qquad$ $17^{50} \pmod{101}$

is 17 a QR

$p = 11$, $a = 2$ $\quad$ $p = 1$, $a = 5$

$\left(\frac{2}{11}\right) = -1$ $\quad$ $\left(\frac{5}{11}\right) = 1$

$10! = 1 \cdot 2 \cdot 3 \cdot \boxed{4} \cdot 5 \cdot 6 \cdot \boxed{7} \cdot 8 \cdot 9 \cdot 10 \equiv -1 \pmod{11}$



$4^2 \equiv 5$

$7^2 \equiv 5$

$10! \equiv 5^4 \cdot 4 \cdot 7$

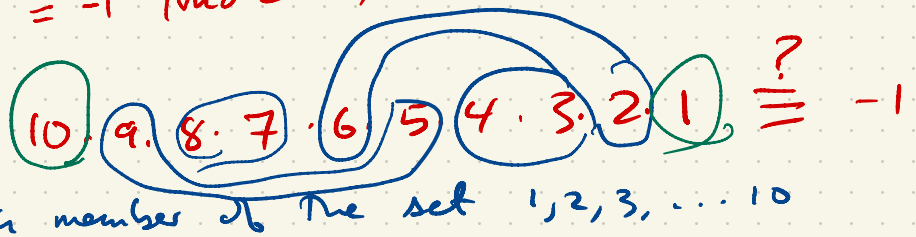
$\equiv 5^4 \cdot 4(-4) \equiv -5^4 \cdot 4^2 \equiv -5^5 \equiv -1$

$5^5 \equiv 1$

$p = 11$

MOD 11

$10! \equiv -1 \pmod{11}$



Each member of the set $1, 2, 3, \ldots 10$ has a MULT INV mod 11

If you are weird $x^2 \equiv 1$

$\Rightarrow x^2 - 1 \equiv 0$

$\Rightarrow (x-1)(x+1) \equiv 0$

$p = 11$ what are the QRS (MOD 11)

$1^2 \equiv 1 \longrightarrow$ 1 is QR $\quad \left(\frac{1}{11}\right) = 1$

$2^2 \equiv 4$. 4

$3^2 \equiv 9$.

$4^2 \equiv 5$

$5^2 \equiv 3$.

$6^2 \equiv (-5)^2 = 5^2 \equiv 3$

$x^2 \equiv a \pmod{11}$

has either 0 or 2 solutions

Suppose $x^2 \equiv a$ and $y^2 \equiv a$

$x^2 - y^2 \equiv 0$

$(x+y)(x-y) \equiv 0$

$x+y \equiv 0$ or $x \equiv y$