Character Sums

Grace Howard

June 2024

Definition 0.1. Let n be a positive integer. For $q \in \{0, 1, 2, \ldots, n-1\}$, q is a quadratic residue modulo n if there exists an integer x such that $x^2 \equiv q \pmod{n}$. Otherwise, q is a quadratic non-residue.

Example

For $n = 5$,

- $0^2 = 0 \equiv 0 \pmod{5}$,
- $1^2 = 1 \equiv 1 \pmod{5}$,
- $2^2 = 4 \equiv 1 \pmod{5}$,
- $3^2 = 9 \equiv 4 \pmod{5}$,

and

- $4^2 = 16 \equiv 1 \pmod{5}$.

So, the quadratic residues are $\{0, 1, 4\}$ and the quadratic non- residues are $\{2, 3\}$.

Theorem 0.1. For $n = p$, where p is an odd prime, there are $\frac{p+1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues.

Proof. Firstly, 0 is always a quadratic residue modulo p since $0^2 = 0 \equiv 0 \pmod{p}$. Thus, there is a need to prove that of the $p-1$ integers relatively prime to p, $\frac{p-1}{2}$ of them are quadratic residues and $\frac{p-1}{2}$ of them are not. Each congruence $x^2 \equiv a \pmod{p}$ has either two or zero solutions and the total set

of solutions has size $p-1$. So, since every number has exactly one square it solves exactly one of these congruences. From this, it must be the case that $\frac{p-1}{2}$ of the congruences have 2 solutions each and the other $\frac{p-1}{2}$ of them have no solutions. $\square$

Definition 0.2. A Dirichlet character modulo q is a function $\chi : \mathbb{Z} \to \mathbb{C}$ such that χ satisfies:

- For all $n \in \mathbb{Z}$, $\chi(n+q) = \chi(n)$,
- for all $n, k \in \mathbb{Z}$, $\chi(nk) = \chi(n)\chi(k)$,

and

- $\chi(n) \neq 0$ if and only if $\gcd(n, q) = 1$.

Definition 0.3. The principal character modulo q is the Dirichlet character χ_1 such that $\chi_1(n) = 1$ if and only if $\gcd(n, q) = 1$.

Definition 0.4. The Legendre symbol is a function of a and p, where p is an odd prime, defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a square} \mod p \\ -1 & \text{if } a \text{ is a quadratic non-residue} \mod p. \end{cases}$$

It has the following properties:

- $\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right)$ for all a,
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ for all a, b,

and

- $\left(\frac{a}{p}\right) \neq 0$ if and only if $\gcd(a, p) = 1$.

By definition, the Legendre symbol is a Dirichlet character.

Let $g(p) = m$ be the least quadratic nonresidue modulo p. Suppose $\chi(a) = \left(\frac{a}{p}\right)$. Then, $\chi(n) = 1$ for $n = 1, 2, \ldots, m-1$ and $\chi(m) = -1$. Therefore,

$$\sum_{i=1}^{m} \chi(m) = \chi(1) + \chi(2) + \cdots + \chi(m-1) + \chi(m) = m - 2$$

and

$$\sum_{i=1}^{k} \chi(i) = k$$

for all $k < m$.

Theorem 0.2. Let q be an integer with $q \geq 2$ and let χ be a non-principal character modulo q. For integers M, N with $N \geq 1$,

$$\left| \sum_{a=M+1}^{M+N} \chi(a) \right| < 3\sqrt{q} \log q.$$

The sum $\sum_{a=M+1}^{M+N} \chi(a)$ is at most N. So, this estimate is non-trivial only if $N > 3\sqrt{q} \log q$. The proof of this theorem relies on two lemmas.

Definition 0.5. $\overline{\chi(a)}$ is the complex conjugate of $\chi(a)$.

Definition 0.6. Let $q \in \mathbb{Z}$ with $q \geq 2$. For a character $\chi \mod q$ and for $b \in \mathbb{Z}$, define the Gauss sum

$$\tau(b, \chi) = \sum_{a \in S_q} \chi(a) e^{2\pi i b a/q}$$

where S_q is a full system of representative modulo q.

Lemma 0.3. Let $q \in \mathbb{Z}$ with $q \geq 2$ and let χ be a character modulo q. Additionally, let $b \in \mathbb{Z}$. Then,

- If $\gcd(b, q) = 1$, then $\tau(b, \chi) = \overline{\chi(b)} \cdot \tau(1, \chi)$.
- If $\gcd(b, q) > 1$ and χ is primitive, then $\tau(b, \chi) = \overline{\chi(b)} \cdot \tau(1, \chi) = 0$.

Lemma 0.4. Let $0 < x < 1$. Then

$$\left| \sum_{a=M+1}^{M+N} e^{2\pi i a x} \right| \leq \frac{1}{2} \max\left(\frac{1}{x}, \frac{1}{1-x} \right).$$

Proof. By the formula for the sum of a geometric series,

$$\begin{aligned} \sum_{a=M+1}^{M+N} e^{2\pi i a x} &= e^{2(M+1)\pi i x} \cdot \frac{e^{2\pi i N x} - 1}{e^{2\pi i x} - 1} \\ &= e^{\pi i (2M+N+1)x} \left(\frac{e^{\pi i N x} - e^{-(\pi i N x)}}{e^{\pi i x} - e^{-(\pi i x)}} \right) \\ &= e^{\pi i (2M+N+1)x} \frac{\sin(N\pi x)}{\sin(\pi x)}. \end{aligned}$$

Firstly, $|e^{\pi y i}| = 1$ and $|\sin(\pi y)| \leq 1$ for every $y \in \mathbb{R}$. Additionally, consider that

$$\sin(\pi x) \geq 2 \min(x, 1-x)$$

for every x with $0 \leq x \leq 1$. □

Definition 0.7. Suppose χ is a character mod q and χ' is a character mod d, where $d > 0$ is a divisor of q. Then, χ is induced by χ' if $\chi(a) = \chi'(a)$ for every $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$.

Definition 0.8. The conductor of χ is the smallest positive divisor d of q such that χ is induced by a character modulo d.

Proof of Theorem 1.2. Suppose that χ is a primitive character modulo q. Then, by

$$\begin{aligned} \sum_{a=M+1}^{M+N} \overline{\chi(a)} &= \tau(1,\chi)^{-1} \sum_{a=M+1}^{M+N} \tau(a,\chi) \\ &= \tau(1,\chi)^{-1} \sum_{a=M+1}^{M+N} \left[\sum_{n=1}^{q-1} \chi(n) e^{2\pi i a \frac{n}{q}} \right] = \tau(1,\chi)^{-1} \sum_{n=1}^{q-1} \chi(n) \sum_{a=M+1}^{M+N} e^{2\pi i a \frac{n}{q}}. \end{aligned}$$

Since $|\chi(n)| \leq 1$ for all n,

$$\left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq \frac{1}{\sqrt{q}} \sum_{n=1}^{q-1} \frac{1}{2} \max\left(\frac{1}{\frac{n}{q}}, \frac{1}{1-\frac{n}{q}} \right) \leq \sqrt{q} \sum_{n=1}^{\lfloor \frac{q}{2} \rfloor} \frac{1}{n}.$$

By inspection,

$$\left|\sum_{a=M+1}^{M+N}\chi(a)\right| < \frac{3}{2}\sqrt{q}\log q.$$

For non- primitive characters, let χ be a non-primitive, non-principal character modulo q and let f be the conductor of χ. Then, χ is induced by a primitive character χ' modulo f. Let $q = f \cdot q'$. If $\gcd(a, q') = 1$, then $\gcd(a, f) = \gcd(a, q)$. From this, $\chi(a) = \chi'(a)$. If $\gcd(a, q') > 1$, then $\chi(a) = 0$. From this,

$$\sum_{a=M+1}^{M+N}\chi(a) = \sum_{\substack{a=M+1\\ \gcd(a,q')=1}}^{M+N}\chi'(a).$$

Using properties of μ,

$$\begin{aligned}\sum_{a=M+1}^{M+N}\chi(a) &= \sum_{a=M+1}^{M+N}\chi'(a)\sum_{d|q',d|a}\mu(d)\\ &= \sum_{d|q'}\mu(d)\sum_{\substack{a=M+1\\ a\equiv 0 \pmod d}}\chi'(a)\end{aligned}$$

$$= \sum_{d|q'}\mu(d)\chi'(d)\sum_{\frac{M+1}{d}\le d_1\le\frac{M+N}{d}}\chi'(d)1)$$

where $a = dd_1$. By the above lemma, the inner sum has absolute value at most $\frac{3}{2}\sqrt{f}\log f$. From this,

$$\left|\sum_{a=M+1}^{M+N}\chi(a)\right| \le \frac{3}{2}\tau(q')\sqrt{f}\log f$$

where $\tau(q')$ is the number of divisors of q'. Then,

$$\left|\sum_{a=M+1}^{M+N}\chi(a)\right| < 2\sqrt{q'}\cdot\frac{3}{2}\sqrt{f}\log f \le 3\sqrt{q}\log q.$$

□