A proof of (a special case of) the Pólya-Vinogradov inequality

Idris Mercer, DePaul University, imercer@depaul.edu

Let p be an odd prime, let $\mathbb{Z}_p$ denote the integers mod p, and let $\mathbb{Z}_p^*$ denote the set of nonzero elements of $\mathbb{Z}_p$, so $\left|\mathbb{Z}_p^*\right| = p-1$. Half of the elements of $\mathbb{Z}_p^*$ are squares, and half are nonsquares. (In fact, $\mathbb{Z}_p^*$ is a cyclic group under multiplication, so if we pick a generator g, the squares are the even powers of g and the nonsquares are the odd powers of g.)

For any integer n, the Legendre symbol $(\frac{n}{p})$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a nonzero square mod } p, \\ -1 & \text{if } n \text{ is a nonsquare mod } p, \\ 0 & \text{if } n \equiv 0 \text{ mod } p. \end{cases}$$

This function is an example of a mod p Dirichlet character, so we will write $\chi(n) = (\frac{n}{p})$. Note that we have $\chi(n+p) = \chi(n)$ and $\chi(mn) = \chi(m)\chi(n)$ for all integers m and n.

For example, if $p = 11$, the elements of $\mathbb{Z}_p^*$ can be written $\{\pm1, \pm2, \pm3, \pm4, \pm5\}$, so the nonzero squares mod 11 are

$$(\pm1)^2 = 1,\ (\pm2)^2 = 4,\ (\pm3)^2 = 9,\ (\pm4)^2 = 16 \equiv 5,\ (\pm5)^2 = 25 \equiv 3$$

and we can make the following table.

n	0	1	2	3	4	5	6	7	8	9	10
$\chi(n)$	0	$+1$	-1	$+1$	$+1$	$+1$	-1	-1	-1	$+1$	-1

If we do this for various p, the sequence of $+1$'s and -1's generated by $\chi(n) = (\frac{n}{p})$ usually tends to look random. Informally speaking, we expect the $+1$'s and -1's to 'balance', but sometimes the same sign happens to appear a large number of times in an interval. In the above example, we see that for $n \in \{1, 2, 3, 4, 5\}$, we have $+1$ appearing four times and -1 appearing only once. That is, if $p = 11$, then the sum

$$\sum_{n=1}^{5} \chi(n) = +1 - 1 + 1 + 1 + 1$$

is not much less than the sum of five +1's. What can happen for a general odd prime p? Can our table begin with one of the two signs appearing an unusually large number of times? In other words, can the partial sum

$$\sum_{n=1}^{m} \chi(n)$$

be almost as extreme as the sum of m +1's or m −1's? (Notice that we may as well assume $m < p-1$. We have $\sum_{n=1}^{p} \chi(n) = \sum_{n=1}^{p-1} \chi(n) = 0$ because of the equal number of squares and nonsquares, and then $\sum_{n=1}^{kp} \chi(n) = 0$ by periodicity.) For example, if we look at the first half of our table, can

$$\sum_{n=1}^{(p-1)/2} \chi(n)$$

be very close to $+\frac{p-1}{2}$ or $-\frac{p-1}{2}$? The Pólya-Vinogradov inequality says no. It says that there is a constant C such that for all p, we have

$$\left| \sum_{n=1}^{m} \chi(n) \right| \leq C\sqrt{p} \log p$$

for all m. (In fact, the Pólya-Vinogradov inequality applies to nonprincipal characters other than the Legendre symbol, but I believe that the special case $\chi(n) = (\frac{n}{p})$ adequately illustrates the ideas of the proof.)

How do we prove the Pólya-Vinogradov inequality? In a sense, the difficulty is that although there are many nice properties of sums of the form $\sum_{n=0}^{p-1}$ or $\sum_{n=1}^{p-1}$, a 'partial' sum of the form $\sum_{n=1}^{m}$ may be harder to deal with. We get around this difficulty with the help of Fourier analysis.

Throughout the rest of this paper, p is a fixed odd prime, $\chi(n)$ denotes $(\frac{n}{p})$, and ω denotes $e^{2\pi i/p}$. The symbol $\equiv$ always refers to congruence mod p.

Lemma 1. *For integers k and n, we have*

$$\frac{1}{p} \sum_{j=0}^{p-1} \omega^{j(k-n)} = \begin{cases} 1 & \text{if } k \equiv n, \\ 0 & \text{if } k \not\equiv n. \end{cases}$$

Proof. If $k \equiv n$, then the left side is the average of p copies of 1. If $k \not\equiv n$, then the left side is invariant under multiplication by $\omega^{k-n} \neq 1$. $\square$

If we use Iverson bracket notation, where $[P] = 1$ if the statement P is true, and $[P] = 0$ if the statement P is false, then Lemma 1 can be written

$$[k \equiv n] = \frac{1}{p} \sum_{j=0}^{p-1} \omega^{j(k-n)}.$$

We now observe that if $n \in \{0, 1, \ldots, p-1\}$, then

$$\begin{aligned}
\chi(n) &= \sum_{k=0}^{p-1} [k \equiv n] \chi(k) \\
\implies \sum_{n=1}^{m} \chi(n) &= \sum_{n=1}^{m} \sum_{k=0}^{p-1} [k \equiv n] \chi(k) \\
&= \sum_{n=1}^{m} \sum_{k=0}^{p-1} \frac{1}{p} \sum_{j=0}^{p-1} \omega^{j(k-n)} \chi(k) \\
&= \frac{1}{p} \sum_{j=0}^{p-1} \left(\sum_{n=1}^{m} \sum_{k=0}^{p-1} \omega^{-jn} \omega^{jk} \chi(k) \right) \\
&= \frac{1}{p} \sum_{j=0}^{p-1} \left(\sum_{n=1}^{m} \omega^{-jn} \cdot \sum_{k=0}^{p-1} \omega^{jk} \chi(k) \right).
\end{aligned}$$

Notice that if $j = 0$, we have

$$\sum_{k=0}^{p-1} \omega^{jk} \chi(k) = \sum_{k=0}^{p-1} \chi(k) = 0$$

so we in fact have

$$\sum_{n=1}^{m} \chi(n) = \frac{1}{p} \sum_{j=1}^{p-1} \left(\sum_{n=1}^{m} \omega^{-jn} \cdot \sum_{k=0}^{p-1} \omega^{jk} \chi(k) \right). \tag{1}$$

We now will consider two separate problems: the problem of bounding

$$\sum_{n=1}^{m} \omega^{-jn}$$

and the problem of bounding

$$\sum_{k=0}^{p-1} \omega^{jk} \chi(k).$$

The latter sum is called a 'Gauss sum' and is much studied in number theory. We will deal with the former sum first.

If we define

$$S = \sum_{n=1}^{m} \omega^{-jn} = \omega^{-j} + \omega^{-2j} + \cdots + \omega^{-mj}$$

then we also have

$$\begin{aligned}
\omega^j S &= 1 + \omega^{-j} + \cdots + \omega^{-(m-1)j} \\
S - \omega^j S &= \omega^{-mj} - 1 \\
S &= \frac{\omega^{-mj} - 1}{1 - \omega^j} \\
|S| &= \frac{|\omega^{-mj} - 1|}{|1 - \omega^j|} \leq \frac{2}{|1 - \omega^j|}.
\end{aligned}$$

Now observe that

$$\begin{aligned}
\left|1 - \omega^j\right|^2 &= (1 - \omega^j)(\overline{1 - \omega^j}) = (1 - \omega^j)(1 - \omega^{-j}) \\
&= 1 - \omega^j - \omega^{-j} + 1 = 2 - 2\mathrm{Re}(\omega^j) = 2 - 2\cos\left(\frac{2\pi j}{p}\right)
\end{aligned}$$

so

$$\left|1 - \omega^j\right| = \sqrt{2 - 2\cos(2\pi j/p)}.$$

In general, for $t \in [0, \pi]$, one can verify that

$$\cos t \leq 1 - \frac{2t^2}{\pi^2}$$

which rearranges to give

$$\begin{aligned}
2 - 2\cos t &\geq \frac{4t^2}{\pi^2} \\
\sqrt{2 - 2\cos t} &\geq \frac{2t}{\pi} \\
\frac{1}{\sqrt{2 - 2\cos t}} &\leq \frac{\pi}{2t}.
\end{aligned}$$

If $j \in \{1, \ldots, \frac{p-1}{2}\}$, then the angle $\frac{2\pi j}{p}$ is in $[0, \pi]$, and we can say

$$|S| \le \frac{2}{|1-\omega^j|} = \frac{2}{\sqrt{2 - 2\cos(\frac{2\pi j}{p})}} \le \frac{2\pi}{2(\frac{2\pi j}{p})} = \frac{p}{2j}. \tag{2}$$

If, however, $j \in \{\frac{p+1}{2}, \ldots, p-1\}$, then we can write $j = p - j'$ for some $j' \in \{1, \ldots, \frac{p-1}{2}\}$, so the angle $\frac{2\pi j'}{p}$ is in $[0, \pi]$, and we have

$$|S| \le \frac{2}{|1-\omega^j|} = \frac{2}{|1-\omega^{p-j'}|} = \frac{2}{|1-\omega^{-j'}|} = \frac{2}{|1-\omega^{j'}|} \le \frac{p}{2j'}. \tag{3}$$

We now consider the problem of bounding or evaluating the Gauss sum

$$G_j = \sum_{k=0}^{p-1} \omega^{jk}\chi(k)$$

where $j \neq 0$. (We already observed that $G_0 = 0$.) Since $\chi(0) = 0$, we have

$$G_j = \sum_{k=1}^{p-1} \omega^{jk}\chi(k).$$

Now observe that if $j \in \{1, \ldots, p-1\}$, we have

$$\chi(j)G_j = \sum_{k=1}^{p-1} \omega^{jk}\chi(k)\chi(j) = \sum_{k=1}^{p-1} \omega^{jk}\chi(jk).$$

Since $j \in \mathbb{Z}_p^*$, as k goes from 1 to $p-1$, then jk will range through the $p-1$ elements of $\mathbb{Z}_p^*$ in some order. This means that we have

$$\chi(j)G_j = \sum_{k=1}^{p-1} \omega^{jk}\chi(jk) = \sum_{k=1}^{p-1} \omega^{k}\chi(k) = G_1$$

so $G_j = G_1/\chi(j) = G_1 \cdot \chi(j) = \pm G_1$. So if we can bound or evaluate G_1, we can bound or evaluate all the G_j.

The trick now is to consider

$$\sum_{j=0}^{p-1} G_j^2 = \sum_{j=1}^{p-1} G_j^2 = \sum_{j=1}^{p-1} G_1^2 = (p-1)G_1^2.$$

That sum can also be written

$$\begin{aligned}
&\sum_{j=0}^{p-1}\left(\sum_{k=0}^{p-1}\omega^{jk}\chi(k)\cdot\sum_{\ell=0}^{p-1}\omega^{j\ell}\chi(\ell)\right)\\
&=\sum_{j=0}^{p-1}\sum_{k=0}^{p-1}\sum_{\ell=0}^{p-1}\omega^{j(k+\ell)}\chi(k\ell)\\
&=\sum_{k=0}^{p-1}\sum_{\ell=0}^{p-1}\chi(k\ell)\sum_{j=0}^{p-1}\omega^{j(k+\ell)}. \qquad (4)
\end{aligned}$$

By Lemma 1, the sum $\sum_{j=0}^{p-1}\omega^{j(k+\ell)}$ is zero unless $\ell \equiv -k$, in which case it has the value p. It follows that the triple sum (4) is equal to

$$\sum_{k=0}^{p-1}\chi(k\cdot(-k))\cdot p = p\sum_{k=0}^{p-1}\chi(-k^2). \qquad (5)$$

If $k = 0$, then $\chi(-k^2) = 0$, and if $k \neq 0$, then $\chi(-k^2) = \chi(-1)\chi(k^2) = \chi(-1)$. Therefore the sum (5) is equal to

$$p(p-1)\chi(-1)$$

and we conclude that we have

$$\begin{aligned}
(p-1)G_1^2 &= p(p-1)\chi(-1)\\
G_1^2 &= \chi(-1)p
\end{aligned}$$

so G_1 is a complex number of modulus $\sqrt{p}$. (Note that $\chi(-1)$ can be $+1$ or -1, so G_1 can be one of the four numbers $\pm\sqrt{p}$ or $\pm i\sqrt{p}$. In fact, it is possible to determine which of those four values G_1 has, but we do not need that here.) Therefore for each $j \in \{1,\ldots,p-1\}$, G_j is a complex number of modulus $\sqrt{p}$.

The remaining step is to put everything together.

We finally return to estimating the sum (1). We have

$$
\begin{aligned}
\left|\sum_{n=1}^{m}\chi(n)\right| &\le \frac{1}{p}\sum_{j=1}^{p-1}\left(\left|\sum_{n=1}^{m}\omega^{-jn}\cdot\sum_{k=0}^{p-1}\omega^{jk}\chi(k)\right|\right)\\
&= \frac{1}{p}\sum_{j=1}^{p-1}\left(\left|\sum_{n=1}^{m}\omega^{-jn}\right|\cdot\left|\sum_{k=0}^{p-1}\omega^{jk}\chi(k)\right|\right)\\
&= \frac{1}{p}\sum_{j=1}^{p-1}\left(\left|\sum_{n=1}^{m}\omega^{-jn}\right|\cdot\sqrt{p}\right)\\
&= \frac{1}{\sqrt{p}}\sum_{j=1}^{p-1}\left|\sum_{n=1}^{m}\omega^{-jn}\right|\\
&= \frac{1}{\sqrt{p}}\left(\sum_{j=1}^{(p-1)/2}\left|\sum_{n=1}^{m}\omega^{-jn}\right| + \sum_{j=(p+1)/2}^{p-1}\left|\sum_{n=1}^{m}\omega^{-jn}\right|\right).
\end{aligned}
$$

We then use (2) to conclude

$$
\sum_{j=1}^{(p-1)/2}\left|\sum_{n=1}^{m}\omega^{-jn}\right| \le \frac{p}{2}\cdot\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{(p-1)/2}\right)
$$

and we use (3) to conclude

$$
\sum_{j=(p+1)/2}^{p-1}\left|\sum_{n=1}^{m}\omega^{-jn}\right| \le \frac{p}{2}\cdot\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{(p-1)/2}\right).
$$

It follows that we have

$$
\begin{aligned}
\left|\sum_{n=1}^{m}\chi(n)\right| &\le \frac{1}{\sqrt{p}}\cdot\frac{2p}{2}\cdot\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{(p-1)/2}\right)\\
&= \sqrt{p}\cdot\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{(p-1)/2}\right)
\end{aligned}
$$

and the harmonic sum $1+\frac{1}{2}+\cdots+\frac{1}{(p-1)/2}$ can be bounded above by a multiple of $\log p$.