The Polya-Vinogradov inequality

Jordan Bell
jordan.bell@gmail.com
Department of Mathematics, University of Toronto

April 3, 2014

Let $\chi : \mathbb{Z} \to \mathbb{C}$ be a primitive Dirichlet character modulo m. χ being a *Dirichlet character modulo* m means that $\chi(kn) = \chi(k)\chi(n)$ for all k, n, that $\chi(n+m) = \chi(n)$ for all n, and that if $\gcd(n, m) > 1$ then $\chi(n) = 0$. χ being *primitive* means that the conductor of χ is m. The *conductor* of χ is the smallest defining modulus of χ. If m' is a divisor of m, m' is said to be a *defining modulus of* χ if $\gcd(n, m) = 1$ and $n \equiv 1 \pmod{m'}$ together imply that $\chi(n) = 1$. If $n \equiv 1 \pmod{m}$ then $\chi(n) = 1$ (sends multiplicative identity to multiplicative identity), so m is a defining modulus, so the conductor of a Dirichlet character modulo m is less than or equal to m.

We shall prove the Polya-Vinogradov inequality for primitive Dirchlet characters. The same inequality holds (using an O term rather than a particular constant) for non-primitive Dirichlet characters. The proof of that involves the fact [1, p. 152, Proposition 8] that a divisor m' of m is a defining modulus for a Dirichlet character χ modulo m if and only if there exists a Dirichlet character χ' modulo m' such that

$$\chi(n) = \chi_0(n) \cdot \chi'(n) \qquad n \in \mathbb{Z},$$

where χ_0 is the principal Dirichlet character modulo m. (The *principal Dirichlet character modulo* m is that character such that $\chi(n) = 0$ if $\gcd(n, m) > 1$ and $\chi(n) = 1$ otherwise.)

If χ is a Dirichlet character modulo m, define the *Gauss sum* $G(\cdot, \chi) : \mathbb{Z} \to \mathbb{C}$ corresponding to this character by

$$G(n, \chi) = \sum_{k=0}^{m-1} \chi(k) e^{2\pi i k n/m}, \qquad n \in \mathbb{Z}.$$

The *Polya-Vinogradov inequality* states that if χ is a primitive Dirichlet character modulo m, then

$$\left| \sum_{n \le N} \chi(n) \right| < \sqrt{m} \log m.$$

We can write $\chi(n)$ using a Fourier series (the Fourier coefficients are defined on the following line, and one proves that any function $\mathbb{Z}/m \to \mathbb{C}$ is equal to its Fourier series)

$$\chi(n) = \sum_{k=0}^{m-1} \hat{\chi}(k) e^{2\pi ikn/m}.$$

The coefficients are defined by

$$\begin{aligned} \hat{\chi}(k) &= \frac{1}{m}\sum_{n=0}^{m-1} \chi(n) e^{-2\pi ikn/m} \\ &= \frac{1}{m} G(-k,\chi). \end{aligned}$$

We use the fact [1, p. 152, Proposition 9] that for any n we have $G(n,\chi) = \overline{\chi}(n) \cdot G(1,\chi)$. This is straightforward to show if $\gcd(n,m) = 1$, but takes some more work if $\gcd(n,m) > 1$ (to show that $G(n,\chi) = 0$ in that case). Using $G(n,\chi) = \overline{\chi}(n) \cdot G(1,\chi)$, we get

$$\chi(n) = \sum_{k=0}^{m-1} \frac{1}{m} \overline{\chi(-k)} \cdot G(1,\chi) e^{2\pi ikn/m} = \frac{G(1,\chi)}{m} \sum_{k=0}^{m-1} \overline{\chi(-k)} e^{2\pi ikn/m}.$$

Therefore

$$\begin{aligned} \sum_{n=1}^{N} \chi(n) &= \sum_{n=1}^{N} \frac{G(1,\chi)}{m} \sum_{k=0}^{m-1} \overline{\chi(-k)} e^{2\pi ikn/m} \\ &= \frac{G(1,\chi)}{m} \sum_{k=0}^{m-1} \overline{\chi(-k)} \sum_{n=1}^{N} e^{2\pi ikn/m} \\ &= \frac{G(1,\chi)}{m} \sum_{k=1}^{m-1} \overline{\chi(-k)} \sum_{n=1}^{N} e^{2\pi ikn/m}. \end{aligned}$$

Let $f(k) = \sum_{n=1}^{N} e^{2\pi ikn/m}$. Thus

$$\sum_{n=1}^{N} \chi(n) = \frac{G(1,\chi)}{m} \sum_{k=1}^{m-1} \overline{\chi(-k)} f(k),$$

and so (because $|\overline{\chi(-k)}|$ is either 1 or 0 and hence is ≤ 1)

$$\left| \sum_{n=1}^{N} \chi(n) \right| = \frac{|G(1,\chi)|}{m} \sum_{k=1}^{m-1} |f(k)|.$$

We have $f(m-k) = \overline{f(k)}$, so $|f(m-k)| = |f(k)|$. Hence

$$\sum_{k=1}^{m-1} |f(k)| \leq 2 \sum_{1 \leq k \leq m/2} |f(k)|.$$

Moreover, for $1 \leq k \leq m/2$ we have, setting $r = e^{2\pi i k/m}$,

$$|f(k)| = \left| \frac{1 - r^{N+1}}{1 - r} \right| \leq \frac{2}{|1 - r|} = \frac{1}{\sin \frac{\pi k}{m}} \leq \frac{1}{\frac{2}{\pi} \cdot \frac{\pi k}{m}} = \frac{m}{2k}.$$

Therefore,

$$\begin{aligned} \left| \sum_{n=1}^{N} \chi(n) \right| &\leq \frac{|G(1,\chi)|}{m} \cdot 2 \sum_{1 \leq k \leq m/2} |f(k)| \\ &\leq \frac{|G(1,\chi)|}{m} \cdot 2 \sum_{1 \leq k \leq m/2} \frac{m}{2k} \\ &= |G(1,\chi)| \sum_{1 \leq k \leq m/2} \frac{1}{k} \\ &< |G(1,\chi)| \log m. \end{aligned}$$

(If m is large enough. It's not true that $\sum_{1 \leq k \leq m/2} \frac{1}{k} \leq \log(m/2)$, but it is true for large enough m that $\sum_{1 \leq k \leq m/2} \frac{1}{k} < \log m$.)

It is a fact [1, p. 154, Proposition 10] that if χ is a primitive Dirichlet character modulo m and $\gcd(n, m) = 1$ then $|G(n,\chi)| = \sqrt{m}$. Thus

$$\left| \sum_{n=1}^{N} \chi(n) \right| < \sqrt{m} \log m.$$

References

[1] Edmund Hlawka, Johannes Schoißengeier, and Rudolf Taschner, *Geometric and analytic number theory*, Universitext, Springer, 1991, Translated from the German by Charles Thomas.