NOTES ON PRIMES IN ARITHMETIC PROGRESSION

STEVEN J. MILLER

Abstract. The following is a quick set of notes of some properties of Dirichlet characters, in particular, how they are used to prove the infinitude of primes in arithmetic progressions. These notes are from *from An Invitation to Modern Number Theory*, by myself and Ramin Takloo-Bighash. As this is a modified snippet from the book, references to other parts of the book are displayed as ??.

1. Dirichlet Characters

1.1. **Dirichlet Characters.** Let m be a positive integer. A completely multiplicative (see Definition **??**) arithmetic function with period m that is not identically zero is called a **Dirichlet character**. In other words, we have a function $f : \mathbb{Z} \to \mathbb{C}$ such that $f(xy) = f(x)f(y)$ and $f(x + m) = f(x)$ for all integers x, y. Often we call the period m the **conductor** or **modulus** of the character.

Exercise 1.1. *Let χ be a Dirichlet character with conductor m. Prove $\chi(1) = 1$. If χ is not identically 1, prove $\chi(0) = 0$.*

Because of the above exercise, we adopt the convention that a Dirichlet character has $\chi(0) = 0$. Otherwise, given any character, there is another character which differs only at 0.

A complex number z is a **root of unity** if there is some positive integer n such that $z^n = 1$. For example, numbers of the form $e^{2\pi ia/q}$ are roots of unity; if a is relatively prime to q, the smallest n that works is q, and we often say it is a q^{th} **root of unity**. Let

$$\chi_0(n) \;=\; \begin{cases} 1 & \text{if } (n, m) = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

We call χ_0 the **trivial** or **principal character** (with conductor m); the remaining characters with conductor m are called **non-trivial** or **non-principal**.

Exercise 1.2. *Let χ be a non-trivial Dirichlet character with conductor m. Prove that if $(n, m) = 1$ then $\chi(n)$ is a root of unity, and if $(n, m) \neq 1$ then $\chi(n) = 0$.*

Theorem 1.3. *The number of Dirichlet characters with conductor m is $\phi(m)$.*

Proof. We prove the theorem for the special case of m prime. By Theorem **??** the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, generated by some g of order $p - 1$. Thus any $x \in (\mathbb{Z}/p\mathbb{Z})^*$ is equivalent to g^k for some k depending on x. As $\chi(g^k) = \chi(g)^k$, once we have determined the Dirichlet character at a generator, its values are determined at all elements (of course, $\chi(0) = \chi(m) = 0$).

By Exercise 1.2, $\chi(g)$ is a root of unity. As $g^{p-1} \equiv 1 \bmod p$ and $\chi(1) = 1$, $\chi(g)^{p-1} = 1$. Therefore $\chi(g) = e^{2\pi ia/(p-1)}$, $a \in \{1, 2, \ldots, p - 1\}$. The proof is completed by noting each of these possible choices of a gives rise to a Dirichlet character, and all the characters are distinct (they have different values at g). □

Not only have we proved (in the case of m prime) how many characters there are, but we have a recipe for them. If $a = p - 1$ in the above proof, we have the trivial character χ_0.

Exercise$^{(h)}$ 1.4 (Important)**.** *Let r and m be relatively prime. Prove that if n ranges over all elements of $\mathbb{Z}/m\mathbb{Z}$ then so does rn (except in a different order if $r \not\equiv 1 \bmod m$).*

Exercise 1.5. *If χ and χ' are Dirichlet characters with conductor m, so is $\chi'' = \chi\chi'$, given by $\chi''(n) = \chi(n)\chi'(n)$. Define $\overline{\chi}(n) = \overline{\chi(n)}$. Prove $\overline{\chi}$ is a Dirichlet character with conductor m, and $\overline{\chi}\chi = \chi_0$.*

Exercise$^{(h)}$ 1.6 (Important)**.** *Prove the Dirichlet characters with conductor m form a multiplicative group with $\phi(m)$ elements and identity element χ_0. In particular, if χ' is a fixed character with conductor m, if χ ranges over all Dirichlet characters with conductor m, so does $\chi'\chi$.*

The following lemma is often called the **orthogonality relations** for characters (orthogonal is another word for perpendicular). See Definition **??** and §**??** for other examples of orthogonality.

Lemma 1.7 (Orthogonality Relations)**.** *The Dirichlet characters with conductor m satisfy*

$$\sum_{n \bmod m} \chi(n) \quad = \quad \begin{cases} \phi(m) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

$$\sum_{\chi \bmod m} \chi(n) \quad = \quad \begin{cases} \phi(m) & \text{if } n \equiv 1 \bmod m \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Proof. We only prove (2) as the proof of (3) is similar. By $\chi \bmod m$ we mean χ ranges over all Dirichlet characters with conductor m. Let r be an integer with $(r, m) = 1$. Then

$$\chi(r) \sum_{n \bmod m} \chi(n) \; = \; \sum_{n \bmod m} \chi(rn) \; = \; \sum_{n \bmod m} \chi(n), \tag{4}$$

as when n ranges over a complete system of residues mod$m$, so does rn (Exercise 1.4). Consequently, denoting the sum in question by S, we have

$$\chi(r)S \; = \; S, \tag{5}$$

implying that $S = 0$ unless $\chi(r) = 1$ for all $(r, m) = 1$ (in this case, χ is the trivial character χ_0, and $S = \phi(m)$). This finishes the proof. □

Exercise$^{(h)}$ 1.8. *Prove* (3)*.*

Exercise 1.9. *Give an alternate proof of* (2) *and* (3) *by using the explicit formulas for the characters χ with prime conductors. Specifically, for any character χ of prime conductor p with g a generator of $(Z/p\mathbb{Z})^*$ there is an a such that $\chi(g) = e^{2\pi i a/(p-1)}$.*

Another useful form of the orthogonality relations is

Exercise 1.10 (Orthogonality Relations)**.** *Show Lemma 1.7 implies*

$$\frac{1}{\phi(m)} \sum_{n \bmod m} \chi(n)\overline{\chi'}(n) \; = \; \begin{cases} 1 & \text{if } \chi' = \chi \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

To each character χ we can associate a vector of its values

$$\vec{\chi} \; \longleftrightarrow \; (\chi(1), \; \chi(2), \; \ldots, \; \chi(m-1), \; \chi(m)), \tag{7}$$

and we may interpret (6) *as saying $\vec{\chi}$ is perpendicular to $\vec{\chi'}$, where the dot product is*

$$\langle \vec{\chi}, \vec{\chi'} \rangle \; = \; \sum_{n \bmod m} \chi(n)\overline{\chi'}(n). \tag{8}$$

Exercise 1.11. *Given n and a integers, prove*

$$\frac{1}{\phi(m)} \sum_{\chi \bmod m} \overline{\chi}(a)\chi(n) \; = \; \begin{cases} 1 & \text{if } n \equiv a \bmod m \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

This exercise provides a way to determine if $a \equiv n \bmod m$.

1.2. **L-functions and Primes in Arithmetic Progressions.** The L-function of a general Dirichlet character with conductor m is defined by

$$L(s,\chi) \;=\; \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{10}$$

Exercise$^{(h)}$ 1.12. *Prove $L(s,\chi)$ converges for $\Re s > 1$. If $\chi \neq \chi_0$, prove that $L(s,\chi)$ can be extended to $\Re s > 0$.*

As in the case of the Riemann zeta function, we have an **Euler product** defined for $\Re s > 1$:

$$L(s,\chi) \;=\; \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{11}$$

Arguing as in Exercise **??**, for $\Re s > 1$, $L(s,\chi) \neq 0$ (again, this is not obvious from the series expansion).

Exercise$^{(h)}$ 1.13. *Prove* (11).

We sketch how these L-functions can be used to investigate primes in arithmetic progressions (see [Da2, EE, Se] for complete details); another application is in counting solutions to congruence equations in §**??**. For example, say we wish to study primes congruent to a modulo m. Using Dirichlet characters modulo m, by Lemma 1.7 we have (at least for $\Re s > 1$)

$$\begin{aligned} \sum_{\chi \bmod m} \chi(a) L(s,\chi) \quad &= \quad \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{\chi \bmod m} \chi(a)\chi(n) \\ &= \quad \sum_{\substack{n=1 \\ n \equiv a \bmod m}}^{\infty} \frac{\phi(m)}{n^s}. \end{aligned} \tag{12}$$

Thus, by using *all* the Dirichlet characters modulo m, we have obtained a sum over integers congruent to a modulo m. We want to study not integers but primes; thus, instead of studying $\chi(a)L(s,\chi)$ we study $\chi(a)\log L(s,\chi)$ (because of the Euler product, the logarithm of $L(s,\chi)$ will involve a sum over primes).

Similar to the Riemann zeta function, there is a Riemann Hypothesis, the **Generalized Riemann Hypothesis** (GRH), which asserts that all the non-trivial zeros of the L-function $L(s,\chi)$ lie on the line $\Re s = \frac{1}{2}$. This is, of course, beyond the reach of current technology, and if proven will have immense arithmetic implications. In fact, very interesting arithmetic information has already been obtained from progress towards GRH. The following exercise sketches one of these.

Exercise 1.14 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *The purpose of this exercise is sketch the ideas for Dirichlet's Theorem for primes in arithmetic progressions. Suppose for all Dirichlet characters $\chi \neq \chi_0$ modulo m, we have $L(1,\chi) \neq 0$. Then for any $(a,m) = 1$, there are infinitely many prime numbers $p \equiv a \bmod m$.*

(1) *Use the Euler product to prove that for $\Re s > 1$,*

$$\log L(s,\chi) \;=\; \sum_{p} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{k p^{ks}}. \tag{13}$$

(2) *Use Exercise 1.11 to show that*

$$\frac{1}{\phi(m)} \sum_{\chi} \overline{\chi}(a) \log L(s,\chi) \;=\; \sum_{p} \sum_{k=1}^{\infty} \sum_{p^k \equiv a \bmod m} \frac{1}{k p^{ks}}. \tag{14}$$

(3) *Show that the right hand side of* (14) *is*

$$\sum_{p \equiv a \bmod m} \frac{1}{p^s} + O(1) \tag{15}$$

as $s \to 1$ from the right (i.e., $s > 1$ converges to 1, often denoted $s \to 1+$).

(4) *Verify that*

$$L(s,\chi_0) \;=\; \zeta(s)\prod_{p|m}\left(1-\frac{1}{p^s}\right); \tag{16}$$

conclude that $\lim_{s\to 1+} L(s,\chi_0) \;=\; +\infty$.

(5) *Show that if for all* $\chi \neq \chi_0$, $L(1,\chi)\neq 0$, *then*

$$\lim_{s\to 1+}\sum_{p\equiv a \bmod m}\frac{1}{p^s} \;=\; \infty, \tag{17}$$

which of course implies there are infinitely many primes congruent to a *modulo* m. *Proving* $L(1,\chi)\neq 0$ *is the crux of Dirichlet's proof; see* [Da2, EE, IR, Se] *for details.*

Exercise 1.15. *The previous exercise allows us to reduce the question on whether or not there are infinitely many primes congruent to* a *modulo* m *to evaluating a finite number of* L*-functions at 1; thus any specific case can be checked. For* $m=4$ *and* $m=6$, *for each character* χ *use a good numerical approximation to* $L(1,\chi)$ *to show that it is non-zero. Note if one has a good bound on the tail of a series it is possible to numerically approximate an infinite sum and show it is non-zero; however, it is not possible to numerically prove an infinite sum is exactly zero.*

Exercise 1.16. *In the spirit of the previous problem, assume we know an infinite sum is rational and we know the denominator is at most* Q. *Prove that if we can show that* $|\sum_{n=1}^{\infty} a_n - 0| < \frac{1}{Q}$ *then this estimate improves itself to* $\sum_{n=1}^{\infty} a_n = 0$. *Unfortunately, it is difficult in practice to prove a sum is rational and to bound the denominator, though there are some instances involving* L*-functions attached to elliptic curves where this can be done. What is more common is to show a sum is a non-negative integer less than* 1, *which then implies the sum is* 0. *We shall see numerous applications of this in Chapter* **??** *(for example §**??**, where we prove* e *is irrational and transcendental).*

Exercise$^{(\mathbf{hr})}$ 1.17. *The difficult part of Dirichlet's proof is showing* $L(1,\chi)\neq 0$ *for real characters* χ; *we show how to handle the non-real characters (this means* $\overline{\chi}\neq\chi$; *for example, the Legendre symbol is a real character). Using* $a=1$ *in Exercise 1.14, show*

$$\sum_{\chi}\log L(\sigma,\chi) \;\geq\; 0 \tag{18}$$

for real $\sigma\geq 1$; *note this sum may be infinite. Therefore* $\prod_{\chi} L(\sigma,\chi)\geq 1$ *for* $\sigma\geq 1$. *Show that if* $L(1,\chi)=0$ *so too does* $L(1,\overline{\chi})$. *Show for a non-real character* χ *that* $L(1,\chi)\neq 0$.

Exercise 1.18. *We saw in Exercise* **??** *that for certain choices of* m *and* a *it is easy to prove there are infinitely many primes congruent to* a *modulo* m. *Modifying Euclid's argument (Theorem* **??***), prove there are infinitely many primes congruent to* -1 *modulo* 4. *Can you find an* a *modulo* 5 *(or* 6 *or* 7*) such that there are infinitely many primes? See* [Mu1] *for how far such elementary arguments can be pushed.*

Remark 1.19. One can show that, to first order, $\pi_{m,a}(x)\sim\frac{\pi(x)}{\phi(m)}$, where $\pi_{m,a}(x)$ is the number of primes at most x congruent to a modulo m. We can see evidence of this in (14). The left hand side of that equation depends very weakly on a. The contribution from the non-principal characters is finite as $s\to 1$; thus the main contribution comes from $\chi_0(a)L(s,\chi_0)=L(s,\chi_0)$. Therefore the main term in (15), $\sum_{p\equiv a \bmod q} p^{-s}$, has a similar $s\to 1$ limit for all a; specifically, the piece that diverges, diverges at the same rate for all a relatively prime to q. The behavior of the correction terms exhibit interesting behavior: certain congruence classes seem to have more primes. See [EE, RubSa].

Exercise 1.20. *By Exercise 1.21 or* **??**,

$$\frac{\pi}{4} \;=\; \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{2n-1}. \tag{19}$$

Note π is irrational (see [NZM]*, page 309). Define*

$$\chi_4(n) \;=\; \begin{cases} (-1)^{(n-1)/2} & \text{if } n \text{ is odd} \\ 0 & \text{otherwise.} \end{cases} \tag{20}$$

Prove χ_4 is a Dirichlet character with conductor 4. By evaluating just $L(1,\chi_4)$ and noting π is irrational, show there are infinitely many primes; we sketch a proof of the irrationality of π^2 in Exercise **??**. *This is another special value proof and provides no information on the number of primes at most x. Using this and properties of $\zeta(s)$, can you deduce that there are infinitely many primes congruent to 1 modulo 4 or -1 modulo 4? Infinite products of rational numbers can be either rational or transcendental; see Exercise* **??**.

Exercise$^{(hr)}$ 1.21 (Gregory-Leibniz Formula)**.** *Prove*

$$\frac{\pi}{4} \;=\; \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1}. \tag{21}$$

Exercise$^{(h)}$ 1.22 (Wallis' Formula)**.** *Prove*

$$\frac{2}{\pi} \;=\; \frac{1}{2}\cdot\frac{3\cdot 3}{2\cdot 4}\cdot\frac{5\cdot 5}{4\cdot 6}\cdot\frac{7\cdot 7}{6\cdot 8}\cdots. \tag{22}$$

See Exercise **??** *for more on infinite products and Chapter* 11 *of* [BB] *for more formulas for π. A good starting point is*

$$\begin{aligned} \int_0^{\pi/2} (\sin x)^{2m} dx &= \frac{1\cdot 3\cdot 5\cdots(2m-1)}{2\cdot 4\cdot 6\cdots 2m}\frac{\pi}{2} \\ \int_0^{\pi/2} (\sin x)^{2m+1} dx &= \frac{2\cdot 4\cdot 6\cdots 2m}{1\cdot 3\cdot 5\cdots(2m+1)}. \end{aligned} \tag{23}$$

Index

References

[BB] J. Borwein and P. Borwein, *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*, John Wiley and Sons, New York, 1987.

[Da1] H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, 7th edition, Cambridge University Press, Cambridge, 1999.

[Da2] H. Davenport, *Multiplicative Number Theory*, 2nd edition, revised by H. Montgomery, Graduate Texts in Mathematics, Vol. 74, Springer-Verlag, New York, 1980.

[EE] W. J. Ellison and F. Ellison, *Prime Numbers*, John Wiley & Sons, New York, 1985.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1990.

[Mu1] R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University, (1988), 161–169.

[NZM] I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, New York, 1991.

[RubSa] M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Experiment. Math. **3** (1994), no. 3, 173–197.

[Se] J. P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1996.

Department of Mathematics, Brown University, 151 Thayer Street, Providence, RI 02912
E-mail address: sjmiller@math.brown.edu