The University of Oxford

MSc (Mathematics and Foundations of Computer Science)

Analytic Number Theory

Michaelmas Term 2021

The steps of this mini project are for your guidance; if you wish to take an alternative route to the desired goal, you are free to do so. But, if you follow the suggested route and find yourself unable to carry out any particular step, you may simply assume it so that you can continue with the mini project, but should make this assumption clear in your presentation.

The purpose of this project is to generalize much of the content of the course to the setting of primes in arithmetic progressions.

Definition 1. Let $q \geq 2$ be an integer. A *Dirichlet Character (mod q)* is a function $\chi : \mathbb{N} \to \mathbb{C}$ such that the following three properties hold:

1. χ is a completely multiplicative function (so $\chi(ab) = \chi(a)\chi(b)$).
2. χ is periodic modulo q (so $\chi(n+q) = \chi(n)$).
3. $\chi(n) = 0$ if and only if n is not coprime to q.

Part 1. Let $f : \mathbb{N} \to \{-1, 0, 1\}$ be the function defined by $f(n) = 0$ if $2|n$, $f(n) = 1$ if $n \equiv 1 \pmod 4$ and $f(n) = -1$ if $n \equiv 3 \pmod 4$.

(i) Show that f is a Dirichlet character (mod 4).

(ii) Define $L(s, f) := \sum_{n=1}^{\infty} f(n)n^{-s}$. Does $\lim_{s\to 1^+} L(s, f)$ exist? What about $\lim_{s\to 1^+} \sum_p \frac{f(p)}{p^s}$? If so, is it positive, negative, or zero?

(iii) Show that there are infinitely many primes congruent to 1 mod 4, and also infinitely many primes congruent to 3 mod 4. Using a computer (or looking online), find some numerical data for the number of primes below $10^6, 10^7, 10^8$ etc in these residue classes. By looking at the numerical data, would you say there are more of one than the other?

Part 2. For this part let $q \geq 3$ be a prime. Recall that a *primitive root modulo* q is an integer r such that $r, r^2, \ldots, r^{q-1}$ are all distinct modulo q (and so r generates all of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$).

(i) Show that a Dirichlet character $\chi \pmod q$ is uniquely determined by its value at a primitive root $r \pmod q$. Deduce that $\chi(n)^{q-1} = 1$ for all integers n coprime to q.

(ii) Let r be a primitive root modulo q. Show that for any choice of $\xi \in \mathbb{C}$ with $\xi^{q-1} = 1$, the completely multiplicative function g with $g(r) = \xi$, $g(q) = 0$ and $g(n+q) = g(n)$ for all n is a well-defined Dirichlet character. How many different Dirichlet characters are there $\pmod q$? Do they form a group?

(iii) Let χ_0 be the 'trivial' Dirichlet character $\pmod q$, which has $\chi_0(n) = 1$ if n is coprime to q, and 0 otherwise (i.e. choosing $\xi = 1$). Show that

$$\sum_{a=1}^{q} \chi(a) = \begin{cases} q-1, & \text{if } \chi = \chi_0, \\ 0, & \text{otherwise,} \end{cases}$$

and that

$$\sum_{\chi \pmod q} \chi(a) = \begin{cases} q-1, & a \equiv 1 \pmod q, \\ 0, & \text{otherwise,} \end{cases}$$

and that for b coprime to q

$$\sum_{\chi \pmod q} \chi(a)\overline{\chi(b)} = \begin{cases} q-1, & a \equiv b \pmod q, \\ 0, & \text{otherwise.} \end{cases}$$

(iv) Show that for $\Re(s) > 1$ and a coprime to q

$$\sum_{\substack{n \in \mathbb{N} \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n^s} = \frac{1}{q-1} \sum_{\chi \pmod q} \overline{\chi(a)} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}.$$

(v) Can you write down explicitly the different values taken by the Dirichlet characters mod 5?

Part 3. Let $q \geq 3$ be a prime.

(i) Let $L(s,\chi)=\sum_{n=1}^\infty \chi(n)n^{-s}$. Show that for $\Re(s)>1$

$$\frac{L'(s,\chi)}{L(s,\chi)}=-\sum_{n=1}^\infty \frac{\Lambda(n)\chi(n)}{n^s}.$$

Deduce that $L(s,\chi)$ is non-zero for $\Re(s)>1$.

(ii) Show that if χ_0 is the trivial character $\pmod q$, then

$$L(s,\chi_0)=(1-q^{-s})\zeta(s).$$

deduce that $L(s,\chi_0)$ can be extended to $\Re(s)>0$ with a simple pole $s=1$ (and no other poles).

(iii) Let $\chi\neq\chi_0$ be a non-trivial Dirichlet character $\pmod q$. Produce a bound for $|\sum_{n<x}\chi(n)|$ which doesn't depend on x. What is the best (smallest) bound you can produce? By looking online, what are the best bounds that you are aware of from the literature?

(iv) Using *(iii)* and partial summation, show that $L(s,\chi)$ has an analytic continuation to $\Re(s)>0$, with no poles in this region for any $\chi\neq\chi_0$. Deduce that $L'(s,\chi)/L(s,\chi)$ remains bounded (in terms of q) as $s\to 1^+$, provided $L(1,\chi)\neq 0$.

(v) Deduce that there are infinitely many primes congruent to $a \pmod q$, for any a coprime to q, provided that $L(1,\chi)\neq 0$ for all $\chi \pmod q$.

(vi) Using the explicit Dirichlet characters found in Part 2, can you prove that there are infinitely many primes in each of the residue classes $1,2,3,4 \pmod 5$?

(vii) Try to explain why we bothered to use Dirichlet characters to do all of this, and why we didn't just work with primes in residue classes directly.

It is a result of Dirichlet that $L(1,\chi)\neq 0$ for all Dirichlet characters χ which are not the trivial character, and so in fact there are infinitely many primes which are congruent to $a \pmod q$ for any coprime a and q. In this mini project, we have seen this in the special cases of $q=4$ and $q=5$, and developed some of the key ideas behind this.

`james.maynard@maths.ox.ac.uk`