Lecture 4

Primes in Arithmetic Progressions – Dirichlet's Theorem

Extensions of Euclid's argument establishing the infinitude of primes

Proposition 1: There are infinitely many primes $p \equiv 3 \bmod 4$

Proof: Let $\{p_1, \dots, p_k\}$ be any finite list of primes with $p_j \equiv 3 \bmod 4$.
Consider $N = 4p_1 \cdots p_k - 1$. Since $N > 1$ it has prime divisors, at least one of which must be $\equiv 3 \bmod 4$ (since $N \not\equiv 1 \bmod 4$)
But as $p_j \nmid N$ for all $1 \le j \le k$, this prime is not on original list. $\square$

Exercise (1):

(a) Prove that there are infinitely many primes $p \not\equiv 1 \bmod q$ $(q \geq 3)$.

(b) Prove that if H is a proper subgroup of $(\mathbb{Z}/q\mathbb{Z})^+$, then there are infinitely many primes which are not in H when reduced mod q.

Proposition 2: There are infinitely many primes $p \equiv 1 \bmod 4$.

Proof: We will use the basic number theory fact that

$$-1 \equiv \square \bmod p \iff p \equiv 1 \bmod 4. \quad (*)$$

Now given any $\{p_1, \dots, p_k\}$ list of primes with $p_j \equiv 1 \bmod 4$, we consider

$$N = (2p_1 \cdots p_k)^2 + 1$$

Since $N > 1$, $\exists$ odd prime $p | N \Rightarrow (2p_1 \cdots p_k)^2 \equiv -1 \bmod p$
$\Rightarrow p \equiv 1 \bmod 4$ (by $(*)$).
But $p_i \nmid N$ for all $1 \le j \le k$. $\square$

In fact, we can also establish the following.

<u>Proposition 3</u>: There are infinitely many primes $p \equiv 1 \bmod q$ $(q \geq 2)$.

<u>Proof</u>: Let $\{p_1, \dots, p_k\}$ be any finite list of primes all $\equiv 1 \bmod q$.

Consider the q^{th} cyclotomic polynomial primative q^{th} roots of unity

$$\Phi_q(x) = \prod_{\substack{a=1 \\ (a,q)=1}}^{q} \left(x - e^{2\pi i a/q}\right) \in \mathbb{Z}[x].$$

evaluated at $n = \ell q p_1 \cdots p_k$ with $\ell \in \mathbb{N}$ chosen large enough to ensure that $\Phi_q(n) > 1$. Since the constant coefficients of $\Phi_q(n)$ are ± 1, it follows that

$$\Phi_q(n) \equiv \pm 1 \bmod n \equiv \pm 1 \bmod q \equiv \pm 1 \bmod p_j, \quad 1 \leq j \leq k.$$

In particular, $\Phi_q(n)$ is <u>not</u> divisible by any p_j or any prime dividing q.

But as $\Phi_q(n) > 1$ it must have a prime divisor p and since

$$\Phi_q(n) \mid n^q - 1$$

this prime must also divide $n^q - 1$. Note that <u>if</u> order of $n \bmod p$ equals q, then we must have $q \mid p-1 \Leftrightarrow p \equiv 1 \bmod q$.

<u>Exercise 2</u>: Show that the order of $n \bmod p$ equals q. $\square$

Naturally, every class $a \bmod q$ with $(a,q)=1$ should contain infinitely many primes.

<u>Theorem 1</u> (Dirichlet) This is the case!

It is to the proof of this Theorem that we now turn our attention.

We deduce Theorem 1 from the following stronger "Mertens-style" result.

<u>Theorem 2</u> For any a with $(a,q)=1$ we have for all $x \geq 2$,

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \log x + O_q(1) .$$

<u>Corollary 1</u>: For any a with $(a,q)=1$ we have for all $x \geq 2$,

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O_q(1)$$

In particular, there are infinitely many primes $p \equiv a \bmod q$.

[Corollary 1 follows from Theorem 2 as in proof of Theorem 3.1 (b)]

In light of Mertens' theorem (Theorem 3.1 (a) & (b)), we can view these results as equidistribution statements, asserting that (in a peculiar average sense) the fraction of the primes falling into a given coprime residue class is exactly $1/\varphi(q)$.

<u>Exercise 3</u>: Show that if $\pi(x;q,a) := \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} 1 \sim c \frac{x}{\log x}$ then c must equal $1/\varphi(q)$.

<u>Hint</u>: Show that of some $M>1$, $\pi(Mx;q,a) - \pi(x;q,a) \gg \frac{x}{\log x}$ for all $x \geq 2$.

Conclude from this that $\pi(x;q,a) \gg_{a,q} \frac{x}{\log x}$

Then argue as in proof of Theorem 3.2.

Proof of Theorem 2

By the orthogonality of Dirichlet characters modulo q (Corollary 1 in Supplement 1)

$$\sum_{\substack{n\le x \\ n\equiv a \bmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a) \left(\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} \right) \qquad (*)$$

Lemma 1: $\displaystyle\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} = \delta_\chi \log x + O_q(1)$

where

$$\delta_\chi = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \ne \chi_0 \text{ and } L(1,\chi)\ne 0 \\ -1 & \text{o/w} \end{cases}$$

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \longleftarrow \text{Dirichlet L-series (associated to } \chi)$$

Setting $a=1$ and plugging Lemma 1 into $(*)$ gives

$$\sum_{\substack{n\le x \\ n\equiv 1 \bmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \left(\sum_{\chi} \delta_\chi \right) \log x + O_q(1)$$

Hence $\sum_{\chi} \delta_\chi \geq 0$. This show that there is at most one character $\chi \ne \chi_0$ with $L(1,\chi)=0$. (Since if such a χ does exist, it must be real because $L(1,\chi)=0$ implies $L(1,\overline{\chi})=0$).

Lemma 2: If $\chi \ne \chi_0$ is real, then $L(1,\chi)\ne 0$

Lemmas 1 & 2 together imply Theorem 1, it also establishes

Theorem 3 (Dirichlet) If $\chi \ne \chi_0$, then $L(1,\chi)\ne 0$.

* This is far from the most elegant way to prove Theorem 3 ...

Proof of Lemma 1

- Suppose $\chi = \chi_0$: Since $\sum_{n\le x} \frac{\Lambda(n)}{n} = \log x + O(1)$ and

$$\sum_{n\le x} \frac{\Lambda(n)}{n} - \sum_{n\le x} \frac{\chi_0(n)\Lambda(n)}{n} = \sum_{p\mid q} \sum_{\substack{p^k\le x\\ k\ge 1}} \frac{\log p}{p^k} \le \sum_{p\mid q} \frac{\log p}{p-1} = O_q(1)$$

$$\Rightarrow \sum_{n\le x} \frac{\chi_0(n)\Lambda(n)}{n} = \log x + O_q(1)$$

$\square$

- Suppose $\chi \ne \chi_0$ & $L(1,\chi)\ne 0$:

Sublemma 1: Let $\chi \ne \chi_0$, then $\sum_{n>x} \frac{\chi(n)}{n} \le 2\varphi(q)\frac{1}{x} \ll_q \frac{1}{x}$.

Proof: By orthogonality $\sum \chi(n) = 0$ when summed over any block of q consecutive integers, and hence $\left|\sum_{n\le x}\chi(n)\right| \le \varphi(q)$.

Let $S(x) := \sum_{n\le x}\chi(n)$, by partial summation

$$\sum_{n>x} \frac{\chi(n)}{n} = \lim_{y\to\infty}\left(\frac{S(y)}{y} - \frac{S(x)}{x} + \int_x^y \frac{S(t)}{t^2}\,dt\right) = -\underbrace{\frac{S(x)}{x}}_{|\cdot|\le \frac{\varphi(q)}{x}} + \underbrace{\int_x^\infty \frac{S(t)}{t^2}\,dt}_{|\cdot|\le \frac{\varphi(q)}{x}}$$

$\square$

$$\sum_{n\le x} \chi(n)\frac{\log n}{n} = \sum_{n\le x}\chi(n)\frac{1}{n}\sum_{d\mid n}\Lambda(d) \qquad \left[\log n = \sum_{d\mid n}\Lambda(d)\right]$$

$$= \sum_{d\le x}\chi(d)\Lambda(d)d^{-1}\sum_{m\le \frac{x}{d}}\chi(m)m^{-1}$$

$$= \sum_{d\le x}\chi(d)\Lambda(d)d^{-1}\left(L(1,\chi) + O_q\left(\frac{d}{x}\right)\right) \qquad [\text{Sublemma}]$$

$$= L(1,\chi)\sum_{d\le x}\frac{\chi(d)\Lambda(d)}{d} + O_q(1) \qquad [\text{Chebyshev}]$$

The result now follows, since by partial sommation

$$\underbrace{\sum_{n\le x} \chi(n)}_{S(x):=} \frac{\log n}{n} = S(x)\frac{\log x}{x} - \int_1^x S(t)\frac{1-\log t}{t^2}\,dt = O_q(1)$$

since $|S(x)| \le \phi(q)$, $\frac{\log x}{x} \le 1$, and $\int_1^\infty \frac{1-\log t}{t^2}\,dt = O(1)$.

- Suppose $\chi \ne \chi_0$ & $L(1,\chi)=0$:

Sublemma 2: $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{o/w} \end{cases}$ & $\Lambda(n) = -\sum_{d|n} \mu(d)\log d$

where $\mu(d)$ is the Möbius function defined by

$$\mu(d) = \begin{cases} (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{o/w} \end{cases}$$

Proof: Exercise or see Supplement 2 on Möbius inversion.

Since $\sum_{n\le x} \frac{\chi(n)}{n}\Lambda(n) = -\sum_{n\le x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log d$

and $\log x = \sum_{n\le x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log x$

$$\Rightarrow \log x + \sum_{n\le x}\frac{\chi(n)}{n}\Lambda(n) = \sum_{n\le x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log\left(\frac{x}{d}\right)$$

$$= \sum_{d\le n}\mu(d)\frac{\chi(d)}{d}\log\left(\frac{x}{d}\right)\sum_{m\le x/d}\frac{\chi(m)}{m}$$

$$= L(1,\chi)\sum_{d\le x}\mu(d)\frac{\chi(d)}{d}\log\left(\frac{x}{d}\right) + O_q(1).$$

Since $L(1,\chi)=0 \Rightarrow \sum_{n\le x}\frac{\chi(n)}{n}\Lambda(n) = -\log x + O_q(1)$. □

Proof of Lemma 2: (i.e. Nonvanishing of $L(1,\chi)$ for $\chi \neq \chi_0$ and real)

Sublemma 3: Let χ be a real Dirichlet character mod q.

For every $n \in \mathbb{N}$

$$\sum_{d|n} \chi(d) \geq \begin{cases} 1 & \text{if } n \text{ is a perfect square} \\ 0 & \text{for all } n. \end{cases}$$

Proof: The proof of this sublemma is simple. If n is a power of a prime, say $n = p^a$, then the divisors of n are $1, p, p^2, \dots, p^a$ and

$$\sum_{d|n} \chi(d) = \chi(1) + \chi(p) + \cdots + \chi(p^a)$$
$$= \chi(1) + \chi(p) + \cdots + \chi(p)^a.$$

Since χ is real, we have $\chi(p) = 0, 1, \text{or } -1$, and hence

$$\sum_{d|n} \chi(d) = \begin{cases} a+1 & \text{if } \chi(p) = 1 \\ 1 & \text{if } \chi(p) = -1 \text{ and } a \text{ is even} \\ 0 & \text{if } \chi(p) = -1 \text{ and } a \text{ is odd} \\ 1. & \text{if } \chi(p) = 0, \text{ that is } p|q. \end{cases}$$

In general, if $n = p_1^{l_1} \cdots p_k^{l_k}$, then any divisor of n which take the form $p_1^{m_1} \cdots p_k^{m_k}$ with $0 \leq m_j \leq l_j$, $1 \leq j \leq k$. Therefore, the multiplicative property of χ given

$$\sum_{d|n} \chi(d) = \prod_{j=1}^{k} \left(\chi(1) + \chi(p_j) + \chi(p_j)^2 + \cdots + \chi(p_j)^{l_j}\right),$$

and the proof is complete. $\square$

By partial summation and Sublemma 1 we see that

$$L(1,\chi) = \sum_{n\le x} \frac{\chi(n)}{n} + \sum_{n>x} \frac{\chi(n)}{n}$$

$$= \frac{S(x)}{x} + \int_1^x \frac{S(t)}{t^2}\,dt + O_q\left(\tfrac{1}{x}\right)$$

where $S(x) = \sum_{n\le x} \chi(n)$. Since $|S(x)| \le \varphi(q)$ it follows that

$$x\,L(1,\chi) = \int_1^x \Big(\sum_{n\le t} \chi(n)\Big) \frac{x}{t^2}\,dt + O_q(1)$$

$$= \int_1^x \Big(\sum_{n\le t} \chi(n)\Big) \left\lfloor \frac{x}{t} \right\rfloor \frac{1}{t}\,dt + O_q(\log x)$$

$$= \underbrace{\int_1^x \sum_{n\le t} \chi(n) \sum_{a\le x/t} 1 \;\frac{dt}{t}}_{(*)} + O_q(\log x).$$

Exercise 4:

$$(*) = \sum_{an\le x} \chi(n) \int_n^{\frac{x}{a}} \frac{1}{t}\,dt$$

$$= \sum_{an\le x} \chi(n) \log \frac{x}{an}$$

$$= \sum_{N\le x} \Big(\sum_{d\mid N} \chi(d)\Big) \log \frac{x}{N}$$

Sublemma 3

$$\ge \sum_{M\le\sqrt{x}} \log \frac{x}{M^2} \ge 2 \sum_{M\le \sqrt{x}/2} \log \frac{x^{1/2}}{M} = 2\log 2 \left\lfloor \frac{\sqrt{x}}{2} \right\rfloor.$$

Hence for all $x \ge 2$,

$$x\,L(1,\chi) \ge 2\log 2 \left\lfloor \frac{\sqrt{x}}{2} \right\rfloor + O_q(\log x) > 0 \quad (\text{as } x\to\infty) \Rightarrow L(1,\chi) > 0.$$

$\square$