Primes in arithmetic progressions

LMS Summer School 2023

Lewis Combes

University of Sheffield

Arithmetic progressions

An arithmetic progression is a sequence of integers of the form

$$a, a + d, a + 2d, a + 3d, \ldots$$

That is, they are the values of functions of the form $a + dn$ at integers n.

Arithmetic progressions

An arithmetic progression is a sequence of integers of the form

$$a, a + d, a + 2d, a + 3d, \dots$$

That is, they are the values of functions of the form $a + dn$ at integers n.

A **prime in the arithmetic progression** is a prime number p of the form $a + dn$. So, in particular, we have

$$p \equiv a \pmod{d}.$$

Arithmetic progressions

An arithmetic progression is a sequence of integers of the form

$$a, a+d, a+2d, a+3d, \dots$$

That is, they are the values of functions of the form $a + dn$ at integers n.

A **prime in the arithmetic progression** is a prime number p of the form $a + dn$. So, in particular, we have

$$p \equiv a \pmod{d}.$$

A natural immediate question is the following: for a given a and d, how many primes are there in the arithmetic progression $a, a+d, a+2d, a+3d, \dots$?

Some examples

If $a = 1$ and $d = 2$, we get

$$1, 3, 5, 7, 9, 11, 13, 15, 17, \ldots$$

There are infinitely many primes in this arithmetic progression.

Some examples

If $a = 1$ and $d = 2$, we get

$$1, 3, 5, 7, 9, 11, 13, 15, 17, \ldots$$

There are infinitely many primes in this arithmetic progression.

How many primes are there in the arithmetic progression $a, a + d, a + 2d, a + 3d, \ldots$?

Some examples

If $a = 1$ and $d = 2$, we get

$$1, 3, 5, 7, 9, 11, 13, 15, 17, \ldots$$

There are infinitely many primes in this arithmetic progression.

How many primes are there in the arithmetic progression $a, a + d, a + 2d, a + 3d, \ldots$?

If $\gcd(a, d) \neq 1$ then there are NONE.

Primes mod 4

We start with an easy case: $d = 4$. Let's start making a list.

p	2	3	5	7	11	13	17	19	23	29	31	37	41
$p \pmod 4$	2	3	1	3	3	1	1	3	3	1	3	1	1

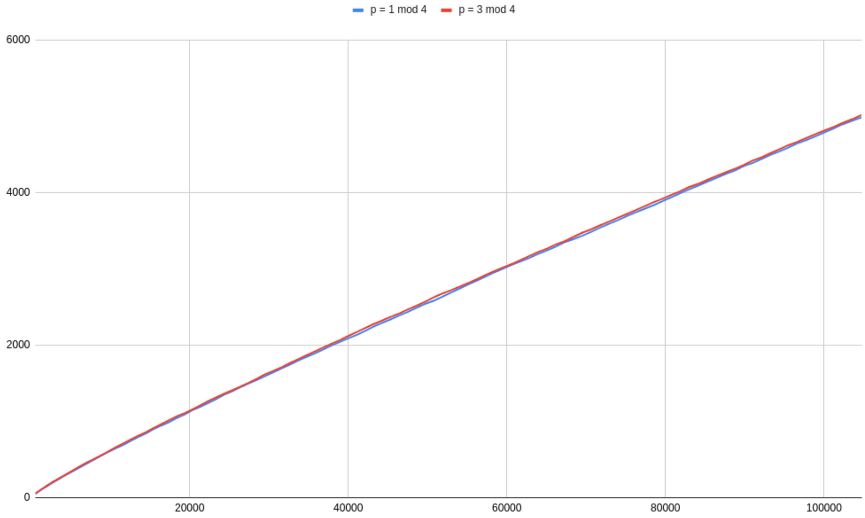
Primes mod 4

We start with an easy case: $d = 4$. Let's start making a list.

p	2	3	5	7	11	13	17	19	23	29	31	37	41
$p \pmod 4$	2	3	1	3	3	1	1	3	3	1	3	1	1

Two important classes: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. With a computer, we can easily find the number of primes of each kind up to various bounds.

Primes mod 4 (cont.)



Primes mod 4 (cont.)

Both classes seem to grow indefinitely. It also seems that there are ever-so-slightly more primes in the 3 class than the 1 class. This leads to some conjectures:

Primes mod 4 (cont.)

Both classes seem to grow indefinitely. It also seems that there are ever-so-slightly more primes in the 3 class than the 1 class. This leads to some conjectures:

Conjecture (Size of classes)

There are infinitely many primes $p \equiv 1, 3 \pmod{4}$.

Primes mod 4 (cont.)

Both classes seem to grow indefinitely. It also seems that there are ever-so-slightly more primes in the 3 class than the 1 class. This leads to some conjectures:

Conjecture (Size of classes)

There are infinitely many primes $p \equiv 1, 3 \pmod 4$.

Conjecture (Ratio of sizes)

Write $P_i(X) = \#\{p \mid p \text{ prime}, p \equiv i \pmod 4, p \leq X\}$. Then

$$\lim_{X \to \infty} \frac{P_1(X)}{P_3(X)} = 1.$$

Primes mod 4 (cont.)

Both classes seem to grow indefinitely. It also seems that there are ever-so-slightly more primes in the 3 class than the 1 class. This leads to some conjectures:

Conjecture (Size of classes)

There are infinitely many primes $p \equiv 1, 3 \pmod 4$.

Conjecture (Ratio of sizes)

Write $P_i(X) = \#\{p \mid p \text{ prime}, p \equiv i \pmod 4, p \leq X\}$. Then

$$\lim_{X \to \infty} \frac{P_1(X)}{P_3(X)} = 1.$$

Conjecture (The race to infinity)

$P_1(X) \leq P_3(X)$ for all $X \in (0, \infty)$.

Size of classes

The first conjecture states that there are infinitely many primes $p \equiv 1, 3 \pmod 4$.

This is TRUE, which we now prove.

Size of classes

The first conjecture states that there are infinitely many primes $p \equiv 1, 3 \pmod 4$.

This is TRUE, which we now prove for primes $p \equiv 3 \pmod 4$.

The case $p \equiv 1 \pmod 4$ works almost the same, but there is a technical hitch that requires some work to solve.

Dirichlet's theorem

Theorem (Dirichlet's theorem on primes in arithmetic progressions)

Let $a, d \in \mathbb{N}$ *such that* $\gcd(a, d) = 1$. *Then there are infinitely many primes* $p \equiv a \pmod{d}$.

Dirichlet's theorem

Theorem (Dirichlet's theorem on primes in arithmetic progressions)

Let $a, d \in \mathbb{N}$ such that $\gcd(a, d) = 1$. Then there are infinitely many primes $p \equiv a \pmod{d}$.

The proof essentially boils down to proving that the sum

$$\sum_{p \equiv a \pmod{d}} \frac{1}{p}$$

diverges. The main techniques are some group theory and some complex analysis.

Dirichlet characters

A **Dirichlet character** is a function $\chi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that

$$\chi(ab) = \chi(a)\chi(b)$$

for all $a, b \in \mathbb{Z}$. We can also think of them as functions $\mathbb{Z} \to \mathbb{C}$ by precomposing with the $\pmod{m}$ map.

Dirichlet characters

A **Dirichlet character** is a function $\chi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that

$$\chi(ab) = \chi(a)\chi(b)$$

for all $a, b \in \mathbb{Z}$. We can also think of them as functions $\mathbb{Z} \to \mathbb{C}$ by precomposing with the $\pmod{m}$ map.

Its L-**function** is the function

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

Dirichlet characters

A **Dirichlet character** is a function $\chi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ such that

$$\chi(ab) = \chi(a)\chi(b)$$

for all $a, b \in \mathbb{Z}$. We can also think of them as functions $\mathbb{Z} \to \mathbb{C}$ by precomposing with the $\pmod{m}$ map.

Its L-**function** is the function

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

Compare this to the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Dirichlet characters (cont.)

The L-function also has an Euler product

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

Dirichlet characters (cont.)

The L-function also has an Euler product

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

Again compare to

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Dirichlet characters mod 4

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

We want to know the values of $L(\chi, 1)$.

Dirichlet characters mod 4

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

We want to know the values of $L(\chi, 1)$.

When $\chi = \chi_1$, we have the identity

$$\begin{aligned} L(\chi_1, s) &= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \ldots \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots - \frac{1}{2^s} - \frac{1}{4^s} - \frac{1}{6^s} \ldots \\ &= \zeta(s) - \frac{1}{2^s}\zeta(s) \\ &= \left(1 - \frac{1}{2^s}\right)\zeta(s) \end{aligned}$$

Dirichlet characters mod 4 (cont.)

Meanwhile,

$$L(\chi_2, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots$$

As $s \to 1$, this approaches the value

$$L(\chi_2, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots =$$

Dirichlet characters mod 4 (cont.)

Meanwhile,

$$L(\chi_2, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots$$

As $s \to 1$, this approaches the value

$$L(\chi_2, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots = \frac{\pi}{4}$$

So $L(\chi_1, 1)$ diverges, and $L(\chi_2, 1)$ converges.

Dirichlet's theorem (again)

Using the Euler product, we get

$$\begin{aligned}\log(L(\chi, s)) &= -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_p \left(\frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{3p^{3s}} + \dots\right) \\ &= \sum_p \frac{\chi(p)}{p^s} + A(\chi, s).\end{aligned}$$

Dirichlet's theorem (again)

Using the Euler product, we get

$$\begin{aligned}\log(L(\chi, s)) &= -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_p \left(\frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{3p^{3s}} + \dots\right) \\ &= \sum_p \frac{\chi(p)}{p^s} + A(\chi, s).\end{aligned}$$

Easy to show that $A(\chi, s)$ is bounded as $s \to 1$.

Dirichlet's theorem (some more)

$$\log(L(\chi, s)) = \sum_p \frac{\chi(p)}{p^s} + A(\chi, s).$$

We note

$$\log(L(\chi_1, s)) + \log(L(\chi_2, s)) = \sum_p \frac{\chi_1(p) + \chi_2(p)}{p^s} + A(\chi_1, s) + A(\chi_2, s).$$

Dirichlet's theorem (some more)

$$\log(L(\chi, s)) = \sum_p \frac{\chi(p)}{p^s} + A(\chi, s).$$

We note

$$\log(L(\chi_1, s)) + \log(L(\chi_2, s)) = \sum_p \frac{\chi_1(p) + \chi_2(p)}{p^s} + A(\chi_1, s) + A(\chi_2, s).$$

$$\chi_1(p) + \chi_2(p) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 4 \\ 0 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Dirichlet's theorem (some more)

$$\log(L(\chi, s)) = \sum_p \frac{\chi(p)}{p^s} + A(\chi, s).$$

We note

$$\log(L(\chi_1, s)) + \log(L(\chi_2, s)) = \sum_p \frac{\chi_1(p) + \chi_2(p)}{p^s} + A(\chi_1, s) + A(\chi_2, s).$$

$$\chi_1(p) + \chi_2(p) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 4 \\ 0 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

So

$$\log(L(\chi_1, s)) + \log(L(\chi_2, s)) = 2 \sum_{p \equiv 1 \pmod 4} \frac{1}{p^s} + A(\chi_1, s) + A(\chi_2, s).$$

Dirichlet's theorem (yet more)

We can also reprove that there are infinitely many primes $\equiv 3 \pmod 4$:

$$\chi_1(p) - \chi_2(p) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4 \\ 2 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Dirichlet's theorem (yet more)

We can also reprove that there are infinitely many primes $\equiv 3 \pmod 4$:

$$\chi_1(p) - \chi_2(p) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4 \\ 2 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

so

$$\log(L(\chi_1, s)) - \log(L(\chi_2, s)) = 2 \sum_{p \equiv 3 \pmod 4} \frac{1}{p^s} + A(\chi_1, s) - A(\chi_2, s).$$

Dirichlet characters mod 5

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	i	$-\mathrm{i}$	-1	0
$\chi_3(n)$	1	-1	-1	1	0
$\chi_4(n)$	1	$-\mathrm{i}$	i	-1	0

Dirichlet characters mod 5

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	i	$-\mathrm{i}$	-1	0
$\chi_3(n)$	1	-1	-1	1	0
$\chi_4(n)$	1	$-\mathrm{i}$	i	-1	0

In a similar way, we have

$$L(\chi_1, 1) = \infty, \quad L(\chi_i, 1) < \infty \text{ for } 2 \le i \le 4.$$

Dirichlet characters mod 5

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	i	$-\mathrm{i}$	-1	0
$\chi_3(n)$	1	-1	-1	1	0
$\chi_4(n)$	1	$-\mathrm{i}$	i	-1	0

In a similar way, we have

$$L(\chi_1, 1) = \infty, \quad L(\chi_i, 1) < \infty \text{ for } 2 \leq i \leq 4.$$

Then we use **orthogonality relations** to pick out individual classes.

Dirichlet characters mod 5

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	i	$-\mathrm{i}$	-1	0
$\chi_3(n)$	1	-1	-1	1	0
$\chi_4(n)$	1	$-\mathrm{i}$	i	-1	0

In a similar way, we have

$$L(\chi_1, 1) = \infty, \quad L(\chi_i, 1) < \infty \text{ for } 2 \leq i \leq 4.$$

Then we use **orthogonality relations** to pick out individual classes. E.g.

$$\chi_1(p) - \mathrm{i}\chi_2(p) - \chi_3(p) + \mathrm{i}\chi_4(p) = \begin{cases} 4 & \text{if } p \equiv 2 \pmod 5 \\ 0 & \text{if } p \not\equiv 2 \pmod 5 \end{cases}$$

Dirichlet characters mod 5

$$\chi_1(p) - \mathrm{i}\chi_2(p) - \chi_3(p) + \mathrm{i}\chi_4(p) = \begin{cases} 4 & \text{if } p \equiv 2 \pmod 5 \\ 0 & \text{if } p \not\equiv 2 \pmod 5 \end{cases}$$

So

$$L(\chi_1, 1) + (\text{other } L\text{-values } < \infty) = 4 \sum_{p \equiv 2 \pmod 5} \frac{1}{p} + (\text{constants})$$

Dirichlet characters mod 5

$$\chi_1(p) - \mathrm{i}\chi_2(p) - \chi_3(p) + \mathrm{i}\chi_4(p) = \begin{cases} 4 & \text{if } p \equiv 2 \pmod 5 \\ 0 & \text{if } p \not\equiv 2 \pmod 5 \end{cases}$$

So

$$L(\chi_1, 1) + (\text{other } L\text{-values } < \infty) = 4 \sum_{p \equiv 2 \pmod 5} \frac{1}{p} + (\text{constants})$$

The method generalises to all moduli d and all residues a to prove

$$\sum_{p \equiv a \pmod d} \frac{1}{p}$$

diverges.

Dirichlet's theorem in general

- $L(\chi_1, 1)$ diverges, the rest converge.
- Orthogonality of characters lets us pick out $\sum_{p \equiv a \pmod{d}} \frac{1}{p}$.
- Connection via Euler product relates the two.

That's it!

Dirichlet's theorem in general

- $L(\chi_1, 1)$ diverges, the rest converge.
- Orthogonality of characters lets us pick out $\sum_{p \equiv a \pmod{d}} \frac{1}{p}$.
- Connection via Euler product relates the two.

That's it*!

The ratio conjecture

We also claimed that

$$\lim_{X\to\infty} \frac{P_1(X)}{P_3(X)} = 1.$$

This is also TRUE. We will not prove it from first principles, as it requires a quite advanced result.

The ratio conjecture

We also claimed that

$$\lim_{X\to\infty} \frac{P_1(X)}{P_3(X)} = 1.$$

This is also TRUE. We will not prove it from first principles, as it requires a quite advanced result.

We define the **density** of a set $S \subset \mathbb{N}$ as

$$D(S) = \lim_{X\to\infty} \frac{\{n \mid n \in S, n \le X\}}{\{n \mid n \in \mathbb{N}, n \le X\}}.$$

So $D(2\mathbb{N}) = \frac{1}{2}$, $D(3\mathbb{N}) = \frac{1}{3}$, ...

The ratio conjecture

We also claimed that

$$\lim_{X \to \infty} \frac{P_1(X)}{P_3(X)} = 1.$$

This is also TRUE. We will not prove it from first principles, as it requires a quite advanced result.

We define the **density** of a set $S \subset \mathbb{N}$ as

$$D(S) = \lim_{X \to \infty} \frac{\{n \mid n \in S, n \leq X\}}{\{n \mid n \in \mathbb{N}, n \leq X\}}.$$

So $D(2\mathbb{N}) = \frac{1}{2}$, $D(3\mathbb{N}) = \frac{1}{3}$, ...

Also, $D(\mathcal{P}) = 0$, where $\mathcal{P}$ is the set of primes.

The ratio conjecture (cont.)

Further, we can define the **relative density** of two sets $S, T \subset \mathbb{N}$ as

$$D(S,T) = \lim_{X\to\infty} \frac{\{n \mid n \in S, n \le X\}}{\{n \mid n \in T, n \le X\}}.$$

So $D(4\mathbb{N}, 2\mathbb{N}) = \frac{1}{2}$, $D(35\mathbb{N}, 5\mathbb{N}) = \frac{1}{7}$,...

The ratio conjecture (cont.)

Further, we can define the **relative density** of two sets $S, T \subset \mathbb{N}$ as

$$D(S,T) = \lim_{X\to\infty} \frac{\{n \mid n \in S, n \le X\}}{\{n \mid n \in T, n \le X\}}.$$

So $D(4\mathbb{N}, 2\mathbb{N}) = \frac{1}{2}$, $D(35\mathbb{N}, 5\mathbb{N}) = \frac{1}{7}, \ldots$

We want to know about the relative densities of subsets of $\mathcal{P}$. Write $S_1 = \{p \equiv 1 \pmod 4\}$, and $S_3 = \{p \equiv 3 \pmod 4\}$. Since

$$S_1 \cap S_3 = \emptyset, \quad S_1 \cup S_3 = \mathcal{P} \backslash \{2\},$$

and we *suspect* that

$$\lim_{X\to\infty} \frac{P_1(X)}{P_3(X)} = 1 \text{ “}=\text{” } \frac{\#S_1}{\#S_3},$$

we predict that $D(S_1, \mathcal{P}) = D(S_3, \mathcal{P}) =$

The ratio conjecture (cont.)

Further, we can define the **relative density** of two sets $S, T \subset \mathbb{N}$ as

$$D(S,T) = \lim_{X\to\infty} \frac{\{n \mid n \in S, n \leq X\}}{\{n \mid n \in T, n \leq X\}}.$$

So $D(4\mathbb{N}, 2\mathbb{N}) = \frac{1}{2}$, $D(35\mathbb{N}, 5\mathbb{N}) = \frac{1}{7}$,...

We want to know about the relative densities of subsets of $\mathcal{P}$. Write $S_1 = \{p \equiv 1 \pmod 4\}$, and $S_3 = \{p \equiv 3 \pmod 4\}$. Since

$$S_1 \cap S_3 = \emptyset, \quad S_1 \cup S_3 = \mathcal{P} \backslash \{2\},$$

and we *suspect* that

$$\lim_{X\to\infty} \frac{P_1(X)}{P_3(X)} = 1 \text{ “}=\text{” } \frac{\#S_1}{\#S_3},$$

we predict that $D(S_1, \mathcal{P}) = D(S_3, \mathcal{P}) = \frac{1}{2}$

Chebotaryov Density

Theorem (Chebotaryov's density theorem)

Writing $S_{a,n}$ for the set of primes congruent to a mod n, we have

$$D(S_{a,n}, \mathcal{P}) = \begin{cases} 0 & \text{if } \gcd(a,n) \neq 1 \\ \frac{1}{\phi(n)} & \text{if } \gcd(a,n) = 1 \end{cases}$$

Here $\phi(n)$ is the **Euler totient function**.

$$\phi(n) = \#\{a \mid 1 \leq a \leq n, \ \gcd(a,n) = 1\}.$$

Chebotaryov Density

Theorem (Chebotaryov's density theorem)

Writing $S_{a,n}$ for the set of primes congruent to a mod n, we have

$$D(S_{a,n}, \mathcal{P}) = \begin{cases} 0 & \text{if } \gcd(a,n) \neq 1 \\ \frac{1}{\phi(n)} & \text{if } \gcd(a,n) = 1 \end{cases}$$

Here $\phi(n)$ is the **Euler totient function**.

$$\phi(n) = \#\{a \mid 1 \leq a \leq n, \ \gcd(a,n) = 1\}.$$

So

$$D(S_1, \mathcal{P}) = D(S_3, \mathcal{P}) = \frac{1}{2}.$$

New prime number theorems

Recall the prime number theorem:

$$\pi(X) = \frac{X}{\log(X)} + E(X)$$

PNT + Dirichlet =

$$\pi(X, 1 \pmod 4) = \frac{1}{2}\frac{X}{\log(X)} + E_1(X)$$

$$\pi(X, 3 \pmod 4) = \frac{1}{2}\frac{X}{\log(X)} + E_3(X)$$

The race to infinity

Recall the conjecture:

Conjecture (The race to infinity)

$P_1(X) \leq P_3(X)$ for all $X \in (0, \infty)$.

The race to infinity

Recall the conjecture:

Conjecture (The race to infinity)

$P_1(X) \leq P_3(X)$ for all $X \in (0, \infty)$.

This is conjecture is FALSE.

The race to infinity

Recall the conjecture:

Conjecture (The race to infinity)

$P_1(X) \leq P_3(X)$ for all $X \in (0, \infty)$.

This is conjecture is FALSE. In fact, it is VERY FALSE. The quantity

$$P_3(X) - P_1(X)$$

changes sign infinitely many times.