1

How many primes end in 7?
Infinitely many, of course! Dirichlet proved a stronger statement:
$\sum_{p\equiv 7 \pmod{10}} \frac{1}{p} \longrightarrow \infty$. More generally:

Thm (Dirichlet, 1837): $\sum_{p\equiv a \pmod{q}} \frac{1}{p} \longrightarrow \infty$ whenever $(a,q)=1$.

Reminiscent of Euler's proof of infinitude of primes using $\zeta(s)$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1-\frac{1}{p^s}\right)^{-1}$$

2

To make this work, Dirichlet introduced $L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$.

For Euler's proof to work, need:
(1) $L(s,\chi)$ has nice analytic properties, i.e. χ behaves nicely.
(2) $L(s,\chi) = \prod_p \left(1-\frac{\chi(p)}{p^s}\right)^{-1}$
i.e. χ is tot. mult.
(3) Want $\chi(p)$ to depend only on $p \pmod q$, not on p!

3

i.e. want $\chi: \mathbb{Z} \longrightarrow \mathbb{C}$ s.t.
- χ is tot. mult. and
- χ is periodic

Propⁿ: Suppose $\chi: \mathbb{Z} \longrightarrow \mathbb{C}$ is
- tot. mult.
- periodic.

Then either $\chi \equiv 0$ or χ is a Dirichlet char.

Pf: We assume $\chi \not\equiv 0$. Thus $\chi(1)=1$.
If $\chi \equiv 1$, done! So assume $\chi \not\equiv 1$.
Thus $\chi(0)=0$.

4

Denote the minimal period of χ by q, and set d to be the maximal divisor of q s.t. $\chi(d) \neq 0$. Then

$$\chi(d)\,\chi(r) = \chi(dr+q) = \chi(d)\chi(r+q/d)$$

for any r. Since $\chi(d) \neq 0$, deduce

$$\chi(r) = \chi(r+q/d) \quad \forall r.$$

$\Rightarrow d=1 \Rightarrow \chi(m) = 0$ iff $(m,q)>1$. ∎

1

In fact, more is true:

Prop (Allouche-G, 2018):

Suppose $\chi: \mathbb{Z} \to \mathbb{C}$ is tot. mult and eventually satisfies a linear recurrence. Then either $\chi \equiv 0$ or χ is a Dirichlet character.

2

In any event, Dirichlet initiated the study of

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

in order to prove his thm. on primes in APs. Recall that convergence properties of $\zeta(s)$ in $\mathbb{C}$ were crucial in proof of PNT. Where does $L(s,\chi)$ converge?

3

Certainly, if $\operatorname{Re} s > 1$, then

$$|L(s,\chi)| \leq \sum \frac{|\chi(n)|}{|n^s|} \leq \sum \frac{1}{n^{\operatorname{Re} s}} < \infty.$$

So $L(s,\chi)$ converges to the right of $\operatorname{Re} s = 1$. What about in the half-plane $\operatorname{Re} s \leq 1$?

The natural tool to use is partial summation (sometimes called Abel summation):

4

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \int_{1^-}^{\infty} \frac{1}{t^s} d\left(\sum_{n \leq t} \chi(n)\right)$$

$$= \frac{1}{t^s} \sum_{n \leq t} \chi(n) \Big|_{1^-}^{\infty} + s \int_1^{\infty} \left(\sum_{n \leq t} \chi(n)\right) \frac{1}{t^{s+1}} dt$$

Lemma: $\forall \chi \neq \chi_0 \pmod q$, $\left|\sum_{n \leq t} \chi(n)\right| \leq q$.

So whenever $\operatorname{Re} s > 0$, 1^{st} term disappears! So, in $\operatorname{Re} s > 0$,

$$L(s,\chi) = s \int_1^{\infty} \frac{1}{t^{s+1}} \left(\sum_{n \leq t} \chi(n)\right) dt.$$

1

We've thus proved:

Prop: $L(s,\chi) = s\int_1^\infty \frac{1}{t^{s+1}}\left(\sum_{n\le t}\chi(n)\right)dt$ when $\mathrm{Re}\, s > 0$.

In particular, $L(s,\chi)$ converges in half-plane $\mathrm{Re}\, s > 0$! This is different from $\zeta(s)$, which blows up @ $s=1$.

Note: The above prop holds for $\chi \neq \chi_0$. We have $L(s,\chi_0) \approx \zeta(s)$.

2

Our proposition shows that if we understand $S_\chi(t)$, then we understand $L(s,\chi)$. Turns out converse also holds!

$$S_\chi(t) = \frac{1}{2\pi i}\int_{(1)} L(s,\chi)\frac{t^s}{s}\,ds$$

Here, (1) can be any line to right of 0, and $t \notin \mathbb{Z}$.

This comes from Perron's formula:

$$\frac{1}{2\pi i}\int_{(\sigma)} \frac{y^s}{s}\,ds = \begin{cases} 0 & 0<y<1 \\ 1/2 & y=1 \\ 1 & y>1 \end{cases}$$

3

The key take-away of all this: understanding $L(s,\chi)$ is, in some sense, equivalent to understanding $S_\chi(t)$. Of course, it's not obvious that $S_\chi(t)$ is an easier object to study!

4

Let's start w/ size of $S_\chi(t)$.

We've already seen:

$$|S_\chi(t)| = \left|\sum_{n\le t}\chi(n)\right| \le q \quad \forall t.$$

What else can we say? When $t<q$,

$$|S_\chi(t)| \le \sum_{n\le t}|\chi(n)| \le t.$$

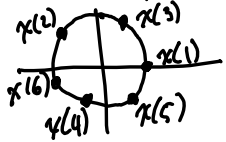
Combining the above two, we have:

Trivial bd: $|S_\chi(t)| \le \max\{t, q\}$.

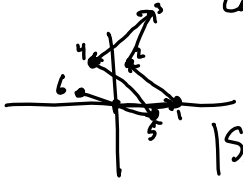
What should we expect?

1

Now $|\chi(n)| = 1$ or 0 $\forall n$, i.e. $\chi(n)$ lives on complex unit circle (or @ 0).



So when you add them up, it's like a random walk in the complex plane.



So maybe reasonable to expect $|S_\chi(t)| \ll \sqrt{t}$?

Let's look @ quite rigorous heuristic:

2

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} |S_\chi(t)|^2 = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \left| \sum_{n \le t} \chi(n) \right|^2$$

$$= \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \sum_{m,n \le t} \chi(m)\overline{\chi(n)}$$

$$= \frac{1}{\varphi(q)} \sum_{\substack{m,n \le t \\ (n,q)=1}} \sum_{\chi \pmod q} \chi(m\bar{n})$$

$$= \sum_{\substack{m,n \le t \\ (n,q)=1 \\ m=n}} 1 = \sum_{\substack{n \le t \\ (n,q)=1}} 1 \approx t.$$

i.e. for typical $\chi \pmod q$, $|S_\chi(t)| \approx \sqrt{t}$.

3

So, might conjecture $|S_\chi(t)| \ll \sqrt{t}$.

This turns out to be false. (We'll see later)

However:

Conjecture (Vinogradov): $S_\chi(t) \ll_\varepsilon \sqrt{t}\, q^\varepsilon$.

Wide open! Known to follow from GRH.

[Note: Harper just proved that for a typical $\chi \pmod q$, $|S_\chi(t)| = o(\sqrt{t})$!]

So, what is known? Sadly, not much.

4

Thm (Pólya-Vinogradov): $\forall \chi \neq \chi_0 \pmod q$,

$$|S_\chi(t)| \ll \sqrt{q} \log q.$$

This is remarkably strong when t is large — almost sqrt cancellation!

But when $t < \sqrt{q} \log q$, this is worse than trivial. In other words, P-V is great when t is huge, terrible when t is small.

1

There's another sense in which P-V isn't terribly shocking. Playing w/ proof of Poisson summation, can show:

Thm ("Twisted Poisson Summation"):

$$\sum_{n \in \mathbb{Z}} f\left(\frac{n}{N}\right) \chi(n) = \hat{\chi}(-1) \cdot N \sum_{\ell \in \mathbb{Z}} \hat{f}\left(\frac{\ell}{qN}\right) \overline{\chi}(\ell)$$

where $\hat{f}$ denotes the fourier transform and $\hat{\chi}(-1) = \frac{\tau(\chi)}{q}$, $\tau(\chi)$ = Gauss sum.

2

Here's a rough interpretation:

$$\left| \sum_{n \le N} \chi(n) \right| \approx \frac{N}{\sqrt{q}} \left| \sum_{\ell \le q/N} \overline{\chi}(\ell) \right| \le \sqrt{q}$$

(trivial if $\ell = 0$!)

This is non-rigorous — Indeed, the conclusion is false!

Thm (Paley, 1932): $\exists$ infty many $\chi \pmod q$ s.t. $\max_t |S_\chi(t)| \gg \sqrt{q} \log\log q$.

3

Paley's result shows Pólya-Vinogradov is close to optimal:

P-V: $\max_t |S_\chi(t)| = O(\sqrt{q} \log q)$

Paley: $\max_t |S_\chi(t)| = \Omega(\sqrt{q} \log\log q)$

It is widely believed that P-V isn't optimal. Here's one piece of evidence:

Thm (Montgomery-Vaughan, '77): Assume GRH. Then $|S_\chi(t)| \ll \sqrt{q} \log\log q$ for all nonprincipal $\chi \pmod q$.

4

In case you're curious about the implicit constant, conjectures exist:

Conjecture: If $\chi \pmod q$ is primitive, then $|S_\chi(t)| \le (C_\chi + o(1)) \sqrt{q} \log\log q$

where $C_\chi = \begin{cases} \frac{e^\gamma}{\pi} & \text{if } \chi = \text{odd} \\ \frac{e^\gamma}{\pi\sqrt{3}} & \text{if } \chi = \text{even}. \end{cases}$

Granville + Soundararajan proved that GRH implies $|S_\chi(t)| \le (2C_\chi + o(1)) \sqrt{q} \log\log q$.

1

Let's compare Pólya-Vinogradov to Vinogradov's conjecture:

P-V: $|S_\chi(t)| \ll \sqrt{q} \log q$

Conj: $|S_\chi(t)| \ll_\varepsilon \sqrt{t}\, q^\varepsilon$.

One obvious difference is that Vinogradov's conjecture depends on t, while P-V doesn't.

2

This explains why P-V can be strong for large t, but worse than trivial for small t. There do exist results that are local rather than global. The strongest of these is due to Burgess:

Thm (Burgess, 1957+...): Given prime p. Then $|S_\chi(t)| \ll_\varepsilon \frac{t}{\log t}$ $\forall t > p^{\frac{1}{4}+\varepsilon}$.

3

By contrast, Vinogradov's conjecture (which, recall, is known to follow from GRH) would imply

$$|S_\chi(t)| \ll_\varepsilon \frac{t}{\log t} \quad \forall t > p^\varepsilon.$$

Unfortunately, Burgess' technique seems hard to improve — his result is a consequence of an analogue of RH for curves over finite fields, which was proved (using

4

difficult methods from algebraic geometry) by Weil. Improving Burgess' bound remains a major open problem w/ many applications throughout number theory.

(It turns out improvements of P-V would imply improvements of Burgess; see Fromm-Goldmakher, Proc. AMS 2019.

1

One final comment on sizes of character sums. Most of our discussion has focused on upper bds. on $S_\chi(t)$; the exception was Paley's result, which showed that $\exists$ infty many $\chi \pmod q$ s.t.

$$|S_\chi(t)| \gg \sqrt{q} \log\log q.$$

One might wonder how rarely

2

character sums get this large. The answer is, very rarely. (See, e.g., Bober-Goldmakher-Granville-Koukoulopoulos, JEMS 2018.)

However, it can be shown w/out much effort that all character sums get almost this large:

Prop: $\forall \chi \pmod q$ primitive,

$$\max_t |S_\chi(t)| \geq \frac{1}{2\pi}\sqrt{q}.$$

3

Proof: Recall that $\forall$ primitive $\chi \pmod q$, the magnitude of the Gauss sum $\tau(\chi)$ is $\sqrt{q}$. Let's apply partial summation to $\tau(\chi)$:

$$\tau(\chi) = \sum_{n \leq q} \chi(n) e\left(\frac{n}{q}\right) = \int_{1^-}^{q} e\left(\frac{t}{q}\right) d S_\chi(t)$$

$$= S_\chi(t) e\left(\frac{t}{q}\right)\Big|_{1^-}^{q} - \int_1^q S_\chi(t)\, e\left(\frac{t}{q}\right)\frac{2\pi i}{q}\, dt$$

4

$$= -\frac{2\pi i}{q}\int_1^q S_\chi(t) e\left(\frac{t}{q}\right) dt.$$

It follows that

$$\sqrt{q} = |\tau(\chi)| \leq \frac{2\pi}{q}\int_1^q |S_\chi(t)|\, dt$$

$$\leq 2\pi \max_t |S_\chi(t)|. \quad \blacksquare$$