We are going to prove Roth's theorem on arithmetic progressions, which is usually proved using Fourier analysis. However, the following proof (from Newman's *Analytic Number Theory*) proves the same theorem using complex analysis and Cauchy's integral formula.

The Theorem

The central question:

> *How 'big' does a set of positive integers have to be before it is guaranteed to have an arithmetic progression?*

First, some questions you might find silly. Is it sufficient for us to say...

Question 1. *...any set of integers that contains more than N elements has a 3-term arithmetic progression, for some N?*

Answer 1. *No...there are infinite sets, like the set of all cubes or the set generated by the greedy algorithm, that are contain no arithmetic progressions.*

Question 2. *...any set of integers that surpasses a certain Lebesgue measure has a 3-term arithmetic progression?*

Answer 2. *No...Lebesgue measure doesn't allow us to distinguish between sizes of sets of integers - they all have Lebesgue measure 0.*

If not, then what's a useful way of distinguishing between sets of natural numbers? It turns out a nice way to classify the 'bigness' of a set of integers A is using the following definition, that is, 'natural density':

$$\text{Density of A} = \limsup_{n\to\infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n}$$

Roughly, this is the probability of encountering an item in the set A within the set of all integers. To get used to this definition...

Question 3. *What is the 'natural density' of any finite set?*

Answer 3. *0*

Question 4. *What is the 'natural density' of the set of odd numbers?*

Answer 4. *1/2*

Question 5. *What is the 'natural density' of the set of prime numbers?*

Answer 5. *0. This is because we know the number of primes less than n is given by $\frac{n}{\log n}$, so* $\lim_{n\to\infty} \frac{n/\log n}{n} = \lim_{n\to\infty} \frac{1}{\log n} = 0.$

It turns out this is a definition that is perfect for our purposes. That is:

Theorem (Roth)
If a set of integers has positive 'natural density,' it must have a 3-term arithmetic progression.

We will spend the rest of this talk proving the contrapositive:

Theorem (Roth)
If a set of integers has no 3-term arithmetic progression, its 'natural density' is 0.

The Proof

So, to prove this theorem, we first want to consider the (not necessarily unique) set

$S(n) :=$ the biggest possible subset of $\{1 \dots n\}$ that has no 3-term arithmetic progressions.

Question 6. *What is $|S(3)|$?*

Answer 6. $|S(3)| = 2$ *since there are only 2 numbers you can take from the set $\{1, 2, 3\}$ without forming a 3-term arithmetic progression.*

Question 7. *What is $|S(5)|$?*

Answer 7. $|S(5)| = 4$ *since the set $\{1, 2, 4, 5\}$ has no 3-term arithmetic progression, but the full set will have an arithmetic progression.*

Then, to prove the theorem, it suffices to show:

$$\text{Density of S} = \limsup_{n\to\infty} \frac{|S(n)|}{n} = 0.$$

That is, if we can show that the density of these maximally-sized AP-free sets is 0, then surely the density of any AP-free set is 0.

Question 8. *What is the relationship between $|S(a+b)|$ and $|S(a)|+|S(b)|$? Is it $=, \leq,$ or $\geq$?*

Answer 8. $|S(a+b)| \leq |S(a)| + |S(b)|$. *That is, $|S(n)|$ is subadditive. We can see this by noticing that if the size $|S(a+b)|$ exceeded $|S(a)|+|S(b)|$, that would mean we should be able to partition $S(a+b)$ into a subset of $\{1,\ldots,a\}$ with no arithmetic progression and a subset of $\{a+1,\ldots,a+b\}$ with no arithmetic progression (and then we can subtract a from each element to get a subset of $\{1,\ldots,b\}$ with no arithmetic progression). At least one of these sets exceeds the size of $|S(a)|$ or $|S(b)|$, which causes a contradiction.*

So, $|S(n)|$ is subadditive. It turns out because the sizes of these sets are subadditive, the limit above actually exists. So rather, all we have to show is:

$$\text{Density of S} = \lim_{n\to\infty} \frac{|S(n)|}{n} = 0$$

And indeed, experimentally, this seems to be true, these sets seem to be getting less dense as n gets bigger:

n	$\lvert S(n)\rvert$	$\lvert S(n)\rvert/n$
1	1	1
2	2	1
4	3	.75
5	4	.80
9	5	$\approx .56$
11	6	$\approx .55$
13	7	$\approx .54$
14	8	$\approx .57$
20	9	$\approx .45$
24	10	$\approx .42$

But, now we have to prove it.

S(n) behaves like a random set

A key fact in proving it will involve figuring out how 'randomly' these extremal sets $S(n)$ behave. So...

Question 9. *For any particular n, do you think the extremal set $S(n)$ has roughly the same number of even and odd elements?*

Answer 9. *It turns out it does. For details of this proof, see appendix lemma A.1.*

As it turns out, $S(n)$ behaves like a random set in the sense it has roughly the same number of odd and even elements, and also in a stronger sense.

$S(n)$ behaves randomly in the sense that its generating function is asymptotically close to the generating function of a random set with the same density (where density is $D = \lim_{n\to\infty} \frac{|S(n)|}{n}$).

$$\sum_{a\in S(n)} z^a = D\sum_{k\le n} z^k + o(n) \qquad \textit{uniformly on } |z| = 1$$

We will prove this by showing that the following polynomial (the difference between the generating function of our extremal set and that of a random set) is small:

$$q(z) = \sum_{a\in S(n)} z^a - D\sum_{k\le n} z^k = o(n)$$

In particular, the way we will do this is by showing that for arbitrary $\epsilon > 0$, $|q(z)| \le 22\epsilon n$.

We know we can bound any n-degree polynomial near a certain point z depending on how it behaves at a nearby point ζ, and how far away it is from that ζ. For a derivation of this, see appendix lemma A.2.

$$|p(z)| \le |\zeta - z| \sum_{m<n} |p_m(\zeta)| + |p(\zeta)|$$

So now we specialize our polynomial as q, and the point we know its behavior at as a root of unity ω. Now, in order to bound $|q(z)|$, we have to bound all the things on the right-hand side here:

$$|q(z)| \le |\omega - z| \sum_{m<n} |q_m(\omega)| + |q(\omega)|$$

It turns out if we choose a new function F and parameter N carefully,[1] the partial sums of our function are pretty tightly bounded at particular roots of unity ω. For details, see appendix A.3.

$$|q_m(\omega)| \le 2\alpha F(\frac{n}{\alpha}) + F(n) \qquad \forall \omega \text{ s.t. } \omega^\alpha = 1, \alpha \le N$$

[1] What is N and F? So first, remember we have let $\epsilon > 0$ be arbitrary. Then we pick a parameter N based on this ϵ. In particular, let $F(x) = \max_{t\le x}(|S(t)| - Dt)$, and since $\frac{F(x)}{x}$ gets arbitrarily small as x goes to infinity, we can always pick an n_0 such that $x \ge n_0$ implies $\frac{F(x)}{x} \le \epsilon$. Then, we pick $N = \lceil \frac{n}{n_0} \rceil$.

Question 10. *Suppose that the choice of ϵ necessitates choosing $N = 3$. For which roots of unity ω does the above bound on $|q_m(\omega)|$ apply?*

Answer 10. *If $N = 3$. the roots of unity ω we are considering are the ω such that $\omega^1 = 1, \omega^2 = 1$, and $\omega^3 = 1$. In particular $\omega = 1, -1, e^{2\pi i/3}, e^{4\pi i/3}$.*

So now we have a bound for $q(z)$ at roots of unity, but want a bound across the entire unit circle. So we need to bound $|\omega - z|$: what's the smallest amount we can stray from each root of unity and still cover the unit circle? Note that the bound on $|q_m(\omega)|$ gets worse as α gets bigger, so ideally we want our bound on $|\omega - z|$ to get smaller as α gets bigger. But just as a first step...

Question 11. *Are all z in the unit circle within $\frac{2\pi}{N}$ from an N^{th} root of unity?*

In other words, fix any z in the unit circle. Is there always an N^{th} root of unity ω (i.e. $\omega^N = 1$) such that z satisfies:

$$|\omega - z| \leq \frac{2\pi}{N}$$

Answer 11. *Yup. We can see in small examples this means that any z in the unit circle is within 2π of any 1st root of unity ($\omega = 1$), always within π of any 2nd root of unity ($\omega = 1, -1$), always within $\frac{2\pi}{3}$ of any 3rd root of unity ($\omega = 1, e^{2\pi i/3}, e^{4\pi i/3}$) and so on.*

And, we can prove this using pigeonhole principle: there are N such roots of unity, and we've divided the circle into N equally sized arcs, so given any point along those arcs, there is going to be a root of unity in that same arc.

But notice that even for small values of N, it seems like this bound is unnecessarily loose. Can we make this bound any tighter?

Question 12. *How can we use Dirichlet's approximation theorem to figure out the smallest amount we can get away from each of those roots of unity (in terms of α and N) and still cover the whole circle?*

Answer 12. *It turns out $|\omega - z| \leq \frac{2\pi}{\alpha(N+1)}$. Details are in appendix B.*

So, it turns out we can travel not too far from each of these particular roots of unity, and still reach all z on the unit circle. We can choose:

$$|\omega - z| \leq \frac{2\pi}{\alpha(N+1)}$$

Plugging those in to the equation above, we can eventually simplify down.

$$\begin{aligned}|q(z)| &\leq |\omega - z| \sum_{m<n} |q_m(\omega)| + |q(\omega)| \\ &\leq \left|\frac{2\pi}{\alpha(N+1)}\right| n|2\alpha F(\frac{n}{\alpha}) + F(n)| + |2\alpha F(\frac{n}{\alpha}) + F(n)| \\ &\ldots \text{lots of calculations which are in the appendix lemma A.4} \ldots \\ &\leq 22\epsilon n\end{aligned}$$

So we have that $|q(z)| \leq 22\epsilon n$ for arbitrary $\epsilon > 0$, so $|q(z)| = o(n)$ as desired. So, the difference between the generating function of our extremal set and a random set is actually quite small.

The number of arithmetic progressions of random sets grows quickly with density

So, now if we can show that dense and random sets have lots of arithmetic progressions, and since our set is random and has no arithmetic progressions, it must not be so dense.

The first thing we do is to find a generating function for our set that somehow tells us the number of arithmetic progressions in the set.

Question 13. *What is a generating function $f(z)$ of a set S that has*

$$A := \textit{the number of arithmetic progressions in } S$$

as its constant term?

For example, if our set $S = \{1, 2, 3\}$ then the constant term of the generating function should be 5, because the arithmetic progressions are $(1,1,1), (2,2,2), (3,3,3), (1,2,3), (3,2,1)$. Note that we count trivial progressions and order.

Hint: Arithmetic progressions (a, b, c) satisfy $a + c = 2b$.

Answer 13. *A is the constant term in the function $f(z) = \sum_{a\in S} z^a \sum_{a\in S} z^a \sum_{a\in S} z^{-2a}$. Why? Note that after multiplying out the three terms in this function, we will only end up with one term of the form $z^1 z^1 z^{-2(1)} = 1$, and one term of the form $z^1 z^3 z^{-2(2)} = 1$, and so on. Every time we end up with a term such that $z^{a+c-2b} = z^0 = 1$, it means we had an a, b, c that satisfied $a + c - 2b = 0$, which means we had another arithmetic progression.*

Now, we want to explicitly find what this constant term of this function $f(z)$ is, without multiplying out the terms. We know we can do this with the Cauchy integral formula for the Laurent series, which tells us for any Laurent series $f(z)$ about a point c, the constant term a_0 is given by:

$$a_0 = \frac{1}{2\pi i} \oint_{|z-c|=r^2} \frac{f(z)}{(z-c)} dz$$

So we can use this to find the number of arithmetic progressions A:

$$A = \frac{1}{2\pi i} \oint_{|z|=1} \frac{\sum_{a \in S(n)} z^a \sum_{a \in S(n)} z^a \sum_{a \in S(n)} z^{-2a}}{z} dz$$

But remember, this generating function is approximately equal to the generating function for a random set when $|z| = 1$, so, it turns out:

$$A = D^3 \left(\frac{1}{2\pi i} \oint_{|z|=1} \frac{\sum_{k \leq n} z^a \sum_{k \leq n} z^a \sum_{k \leq n} z^{-2a}}{z} dz \right) + o(n^2)$$

Question 14. *Without actually calculating the integral or multiplying out the sum, what does the following evaluate to?*

$$\frac{1}{2\pi i} \oint_{|z|=1} \frac{\sum_{k \leq n} z^a \sum_{k \leq n} z^a \sum_{k \leq n} z^{-2a}}{z} dz$$

Answer 14. *With the same generating function logic, the integral counts the number of arithmetic progressions in the set* $\{1 \dots n\}$*, which is* $\frac{n^2}{2}$.

Given the answer above, we can now simplify to:

$$A = \frac{D^3}{2} n^2 + o(n^2)$$

Roughly, the above equation tells us that the number of arithmetic progressions A grows quickly with density.

Conclusion: S(n) can't be dense

Since S(n) has no non-trivial arithmetic progressions, it only has trivial arithmetic progressions, of which there are at most $|S(n)|$. So $A \leq |S(n)| \leq n$. So

$$\frac{D^3}{2} n^2 + o(n^2) \leq n$$

So $D = 0$. That is, extremal sets $S(n)$ with no arithmetic progressions have zero density. And so all sets with no arithmetic progressions have zero density.

A Appendix: Lemmas

Lemma A.1. *For any fixed n, $S(n)$ has roughly the same number of even and odd elements.*

Proof: *Suppose that $S(n)$ has i even elements and j odd elements.*

We could write its even elements like

$$\{2a_1, \ldots, \underbrace{2a_i}_{\leq n}\}.$$

And so then since scaling sets with no APs preserves the fact that it has no AP, the following is an i-element subset of $\{1, \frac{n}{2}\}$ with no AP.

$$\{a_1, \ldots, \underbrace{a_i}_{\leq \frac{n}{2}}\}.$$

So, we conclude $i \leq |S(\frac{n}{2})|$. Since $|S(\frac{n}{2})| \approx \frac{1}{2}|S(n)|$, we have $i \lessapprox \frac{1}{2}|S(n)|$.

We do the same thing with odd elements to find $j \lessapprox \frac{1}{2}|S(n)|$.

So, both even and odd elements take up not much more than half the set.

Lemma A.2. *We can bound any polynomial near a certain point z depending on how it behaves at a nearby point ζ, and how far away it is from that ζ (naturally, the farther it is from that ζ point we know about, the less restricted the bound is):*

$$|p(z)| \leq |\zeta - z| \sum_{m<n} |p_m(\zeta)| + |p(\zeta)|$$

Proof:

Warning: This proof first involves polynomial long division (a series of tedious factoring, multiplying, and substitutions) and finally a taking of absolute values to get the bound.

First, we know we can write any polynomial like:

$$p(z) = \sum_{k=0}^{n} a_k z^k$$

Then we let ζ be some complex constant, and both multiply and divide by it:

$$p(z) = \sum_{k=0}^{n} a_k \left(\frac{z}{\zeta}\right)^k \zeta^k$$

Then we do a change of variables, letting $\omega = \frac{z}{\zeta}$:

$$p(z) = \sum_{k=0}^{n} a_k \omega^k \zeta^k$$

Note this is just a new polynomial in terms of the new variable ω. Let's call it $Q(\omega)$.

$$Q(\omega) = \sum_{k=0}^{n} b_k \omega^k$$

Subtract $Q(1)$ from both sides:

$$\begin{aligned}
Q(\omega) - Q(1) &= \sum_{k=0}^{n} b_k \omega^k - Q(1) \\
&= \sum_{k=0}^{n} b_k \omega^k - \sum_{k=0}^{n} b_k \\
&= \sum_{k=0}^{n} b_k (\omega^k - 1) \\
&= \sum_{k=1}^{n} b_k (\omega^k - 1) \\
&= \sum_{k=1}^{n} b_k (\omega - 1)(\omega^{k-1} + \cdots + 1)
\end{aligned}$$

Then dividing both sides by $\omega - 1$:

$$\begin{aligned}
\frac{Q(\omega) - Q(1)}{\omega - 1} &= \sum_{k=1}^{n} b_k(\omega^{k-1} + \cdots + 1) \\
&= \sum_{k=1}^{n} b_k \sum_{i=0}^{k-1} \omega^i \\
&= \sum_{k=1}^{n} \sum_{i=0}^{k-1} b_k \omega^i \\
&= \sum_{i=0}^{n-1} \sum_{k=i+1}^{n} b_k \omega^i \\
&= \sum_{i=0}^{n-1} \omega^i \sum_{k=i+1}^{n} b_k \\
&= \sum_{i=0}^{n-1} \omega^i \sum_{k=i+1}^{n} b_k \\
&= \sum_{i=0}^{n-1} \omega^i \left(\sum_{k=0}^{n} b_k - \sum_{k=0}^{i} b_k \right) \\
&= \sum_{i=0}^{n-1} \omega^i \left(Q(1) - \sum_{k=0}^{i} b_k \right)
\end{aligned}$$

Multiplying both sides by -1:

$$\frac{Q(\omega) - Q(1)}{1 - \omega} = \sum_{i=0}^{n-1} \omega^i \left(\sum_{k=0}^{i} b_k - Q(1) \right)$$

Moving a term over to the right side:

$$\begin{aligned}
\frac{Q(\omega)}{1 - \omega} &= \sum_{i=0}^{n-1} \omega^i \left(\sum_{k=0}^{i} b_k - Q(1) \right) + \frac{Q(1)}{1 - \omega} \\
&= \sum_{i=0}^{n-1} \omega^i \sum_{k=0}^{i} b_k - \sum_{i=0}^{n-1} \omega^i Q(1) + \frac{Q(1)}{1 - \omega} \\
&= \sum_{i=0}^{n-1} \omega^i \sum_{k=0}^{i} b_k + Q(1) \left(\frac{1}{1 - \omega} - \sum_{i=0}^{n-1} \omega^i \right) \\
&= \sum_{i=0}^{n-1} \omega^i \sum_{k=0}^{i} b_k + Q(1) \left(\frac{1}{1 - \omega} - \frac{1 - \omega^n}{1 - \omega} \right) \\
&= \sum_{i=0}^{n-1} \left(\sum_{k=0}^{i} b_k \right) \omega^i + \frac{Q(1)}{1 - \omega} \omega^n
\end{aligned}$$

To change all the variables back, we notice that:

- $Q(\omega) = \sum_{k=0}^{n} b_k \omega^k = \sum_{k=0}^{n} a_k \omega^k \zeta^k = p(z)$
- $\omega = \frac{z}{\zeta}$
- $\sum_{k=0}^{i} b_k = \sum_{k=0}^{i} a_k \zeta_k = p_i(\zeta)$
- $Q(1) = \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} a_k \zeta_k = p(\zeta)$

Putting these together:

$$\frac{p(z)}{1-\frac{z}{\zeta}} = \sum_{i<n} p_i(\zeta) \left(\frac{z}{\zeta}\right)^i + \frac{p(\zeta)}{1-\frac{z}{\zeta}} \left(\frac{z}{\zeta}\right)^n$$

And when you take absolute values of both sides and apply triangle inequality:

$$\left|\frac{p(z)}{1-\frac{z}{\zeta}}\right| \leq \left|\sum_{i<n} p_i(\zeta) \left(\frac{z}{\zeta}\right)^i\right| + \left|\frac{p(\zeta)}{1-\frac{z}{\zeta}} \left(\frac{z}{\zeta}\right)^n\right|$$

Multiplying both sides by $\left|1-\frac{z}{\zeta}\right|$*:*

$$|p(z)| \leq \left|1-\frac{z}{\zeta}\right| \left|\sum_{i<n} p_i(\zeta) \left(\frac{z}{\zeta}\right)^i\right| + \left|p(\zeta) \left(\frac{z}{\zeta}\right)^n\right|$$

Multiplying both sides by $|\zeta| = 1$*:*

$$|p(z)| \leq |\zeta - z| \left|\sum_{i<n} p_i(\zeta) \left(\frac{z}{\zeta}\right)^i\right| + \left|p(\zeta) \left(\frac{z}{\zeta}\right)^n\right|$$

Applying triangle inequality again, we end up with the desired bound:

$$|p(z)| \leq |\zeta - z| \sum_{i<n} |p_i(\zeta)| + |p(\zeta)|$$

Lemma A.3. *The partial sums of q are bounded near roots of unity ω:*

$$|q_m(\omega)| \leq 2\alpha F(\frac{n}{\alpha}) + F(n)$$

Here, $F = \max_{t \leq x}(|S(t)| - Dt)$ and α has already been determined by the Dirichlet estimate (recall also that $\omega^\alpha = 1$ and $\alpha \leq N$).

Proof:

We know by definition:

$$q(\omega) = \sum_{a \in S(n)} \omega^a - D \sum_{k \leq n} \omega^k$$

So also by definition:

$$q_m(\omega) = \sum_{\substack{a \in S(n) \\ a \leq m}} \omega^a - D \sum_{k \leq m} \omega^k$$

Now we can perform a slightly modified version of Euclidean division, dividing both a and k by α.

- *We write $a = \alpha q_a + r_a$*
- *We write $k = \alpha q_k + r_k$*

This is 'modified' division because we will do it such that the remainder $r \in \{1, \ldots, \alpha\}$ rather than $r \in \{0, \ldots, \alpha - 1\}$. We can do this because both $a > 0$ and $k > 0$ (if not, there would be no way to represent them as a sum of something and some strictly positive remainder).

So:

$$q_m(\omega) = \sum_{\substack{a \in S(n) \\ a \leq m}} \omega^{\alpha q_a + r_a} - D \sum_{k \leq m} \omega^{\alpha q_k + r_k}$$

Now, we can notice that we can sum over all possible values of the remainder $\beta = \{1, \ldots, \alpha\}$, but only count the sum when the remainder r is the correct β.

$$q_m(\omega) = \sum_{\beta=1}^{\alpha} \sum_{\substack{a \in S(n) \\ a \leq m \\ r_a = \beta}} \omega^{\alpha q_a + r_a} - D \sum_{\beta=1}^{\alpha} \sum_{\substack{k \leq m \\ r_k = \beta}} \omega^{\alpha q_k + r_k}$$

$$= \sum_{\beta=1}^{\alpha} \sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} \omega^{\alpha q_a + \beta} - D \sum_{\beta=1}^{\alpha} \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} \omega^{\alpha q_k + \beta}$$

Since $\omega^\alpha = 1$, this simplifies down to:

$$q_m(\omega) = \sum_{\beta=1}^{\alpha} \sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} \omega^\beta - D \sum_{\beta=1}^{\alpha} \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} \omega^\beta$$

$$= \sum_{\beta=1}^{\alpha} \omega^\beta \left(\sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} 1 - D \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} 1 \right)$$

By adding and subtracting the same thing, we get a slightly different form:

$$q_m(\omega) = \sum_{\beta=1}^{\alpha} \omega^\beta \left(\sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} 1 - D \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} 1 + \left| S\left(\frac{m}{\alpha}\right) \right| - \left| S\left(\frac{m}{\alpha}\right) \right| \right)$$

$$= -\sum_{\beta=1}^{\alpha} \omega^\beta \left(\left| S\left(\frac{m}{\alpha}\right) \right| - \sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} 1 \right) + \sum_{\beta=1}^{\alpha} \omega^\beta \left(\left| S\left(\frac{m}{\alpha}\right) \right| - D \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} 1 \right)$$

After applying triangle inequality, we take advantage of the fact that $|\omega| = 1$:

$$|q_m(\omega)| \leq \sum_{\beta=1}^{\alpha} |\omega^\beta| \left| \left| S\left(\frac{m}{\alpha}\right) \right| - \sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} 1 \right| + \sum_{\beta=1}^{\alpha} |\omega^\beta| \left| \left| S\left(\frac{m}{\alpha}\right) \right| - D \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} 1 \right|$$

$$= \sum_{\beta=1}^{\alpha} \left| \left| S\left(\frac{m}{\alpha}\right) \right| - \sum_{\substack{a \in S(n) \\ a \leq m \\ a \equiv \beta mod \alpha}} 1 \right| + \sum_{\beta=1}^{\alpha} \left| \left| S\left(\frac{m}{\alpha}\right) \right| - D \sum_{\substack{k \leq m \\ k \equiv \beta mod \alpha}} 1 \right|$$

And since $\sum_{\substack{k\leq m \\ k\equiv\beta mod\alpha}} 1 = \lceil \frac{m}{\alpha} \rceil \geq \frac{m}{\alpha}$*:*

$$|q_m(\omega)| \leq \sum_{\beta=1}^{\alpha} \left| \left| S\left(\frac{m}{\alpha}\right) \right| - \sum_{\substack{a\in S(n) \\ a\leq m \\ a\equiv\beta mod\alpha}} 1 \right| + \sum_{\beta=1}^{\alpha} \left| \left| S\left(\frac{m}{\alpha}\right) \right| - D\cdot\frac{m}{\alpha} \right|$$

You can show both quantities in the outer absolute value signs are positive, so we can remove those absolute value signs:

$$|q_m(\omega)| \leq \sum_{\beta=1}^{\alpha} \left(\left| S\left(\frac{m}{\alpha}\right) \right| - \sum_{\substack{a\in S(n) \\ a\leq m \\ a\equiv\beta mod\alpha}} 1 \right) + \sum_{\beta=1}^{\alpha} \left(\left| S\left(\frac{m}{\alpha}\right) \right| - D\cdot\frac{m}{\alpha} \right)$$

Doing the summation:

$$|q_m(\omega)| \leq 2\alpha \left| S\left(\frac{m}{\alpha}\right) \right| - \sum_{\beta=1}^{\alpha} \sum_{\substack{a\in S(n) \\ a\leq m \\ a\equiv\beta mod\alpha}} 1 - Dm$$

Then we can notice that:

$$\underbrace{\sum_{\beta=1}^{\alpha} \sum_{\substack{a\in S(n) \\ a\leq m \\ a\equiv\beta mod\alpha}} 1}_{\text{The number of elements in S(n) below m}} \geq \underbrace{|S(n)|}_{\text{The number of elements in S(n)}} - \underbrace{|S(n-m)|}_{\text{An upper bound on the elements in S(n) above m}}$$

So:

$$|q_m(\omega)| \leq 2\alpha \left| S\left(\frac{m}{\alpha}\right) \right| - |S(n)| + |S(n-m)| - Dm$$

Since $D = \lim \frac{|S(n)|}{n} = \inf \frac{|S(n)|}{n} \leq \frac{|S(n)|}{n}$*, we know* $|S(n)| \geq Dn$*:*

$$|q_m(\omega)| \leq 2\alpha \left| S\left(\frac{m}{\alpha}\right) \right| - Dn + |S(n-m)| - Dm$$

After both adding and subtracting $2Dm$ to the right hand side and performing some manipulations:

$$\begin{aligned}|q_m(\omega)| &\leq \left(2\alpha\left|S\left(\frac{m}{\alpha}\right)\right| - 2Dm\right) + (|S(n-m)| - Dn + Dm) \\ &= 2\alpha\left[\left|S\left(\frac{m}{\alpha}\right)\right| - D\cdot\frac{m}{\alpha}\right] + [|S(n-m)| - D\cdot(n-m)]\end{aligned}$$

Now, note that we can find a 'monotone majorant' of anything of the form $|S(x)| - Dx$, since:

$$|S(x)| - Dx \leq \underbrace{\max_{t\leq x}\left[|S(t)| - Dt\right]}_{\text{Call this function F(x)}}$$

So we end up with our desired bound:

$$\begin{aligned}|q_m(\omega)| &\leq 2\alpha F\left(\frac{m}{\alpha}\right) + F(n-m) \\ &\leq 2\alpha F\left(\frac{n}{\alpha}\right) + F(n)\end{aligned}$$

Lemma A.4. *The polynomial q is $o(n)$.*

Proof:

Remember, we start with arbitrary $\epsilon > 0$, and we want to show $|q(z)| \leq 22\epsilon n$.

Because of previous lemmas, we already have that:

$$\begin{aligned}|q(z)| &\leq |\omega - z| \sum_{m<n} |q_m(\omega)| + |q(\omega)| \\ &\leq \left|\frac{2\pi}{\alpha(N+1)}\right| n|2\alpha F(\frac{n}{\alpha}) + F(n)| + |2\alpha F(\frac{n}{\alpha}) + F(n)|\end{aligned}$$

(Annoying parameters debrief). Recall $F(x) = \max_{t \leq x} [|S(t)| - Dt]$, which is monotonic and $\lim_{x\to\infty} \frac{F(x)}{x} = 0$. So since $\frac{F(x)}{x}$ gets arbitrarily small, we can choose an n_0 depending on ϵ such that when $n \geq n_0$ then $\frac{F(n)}{n} \leq \epsilon$. Then we choose $N = \lfloor \frac{n}{n_0} \rfloor$. Finally, since we are trying to prove a statement regarding the limit of n, we can choose n big enough such that $n \geq n_1$, where $n \geq n_1$ implies $\frac{F(n)}{n} \leq \frac{\epsilon}{n_0}$.

Since $N = \lfloor \frac{n}{n_0} \rfloor$, we can apply a few manipulations to find $\frac{1}{N+1} \leq \frac{n_0}{n}$, so:

$$\begin{aligned}|q(z)| &\leq \frac{2\pi n_0}{\alpha}|2\alpha F(\frac{n}{\alpha}) + F(n)| + |2\alpha F(\frac{n}{\alpha}) + F(n)| \\ &= \left[2\alpha F(\frac{n}{\alpha}) + F(n)\right]\left[1 + \frac{2\pi n_0}{\alpha}\right]\end{aligned}$$

Now we apply a case analysis.

Case 1: $\alpha \leq n_0$**.**

$$\begin{aligned}|q(z)| &\leq \left[2\alpha F(\frac{n}{\alpha}) + F(n)\right]\left[1 + \frac{2\pi n_0}{\alpha}\right] \\ &\leq [2\alpha F(n) + F(n)]\left[1 + \frac{2\pi n_0}{\alpha}\right] \qquad \textit{(Since } F(\tfrac{n}{\alpha}) \leq F(n) \textit{ by monotonicity of F)} \\ &= [2\alpha + 1]\left[1 + \frac{2\pi n_0}{\alpha}\right] F(n) \\ &\leq 3\alpha\left[1 + \frac{2\pi n_0}{\alpha}\right] F(n) \\ &\leq 3n_0\left[1 + \frac{2\pi n_0}{n_0}\right] F(n) \qquad \textit{(Since } \alpha \leq n_0 \textit{ by assumption)} \\ &= n_0\left[3 + 6\pi\right] F(n) \\ &= n_0\left[3 + 6\pi\right]\left[\frac{\epsilon n}{n_0}\right] \qquad \textit{(Since } F(n) \leq \frac{\epsilon n}{n_0} \textit{ by case assumption)} \\ &= 22\epsilon n \qquad \textit{(Since } 3 + 6\pi \leq 22\textit{)}\end{aligned}$$

Case 2: $\alpha > n_0$**.**

We know that $x \geq n_0 \implies F(x) \leq \epsilon x$*. We can specialize this to:*

- $\frac{n}{\alpha} \geq n_0 \implies F(\frac{n}{\alpha}) \leq \epsilon \frac{n}{\alpha}$*. Indeed, this is true, since* $\alpha \leq N$ *by Dirichlet, so* $\alpha \leq \frac{n}{n_0}$*.*
- $n \geq n_0 \implies F(n) \leq \epsilon n$*. Indeed, this is also true, since if* $\frac{n}{\alpha} \geq n_0$*, surely* $n \geq n_0$*.*

So now:

$$\begin{aligned}
|q(z)| &\leq \left[2\alpha F(\frac{n}{\alpha}) + F(n)\right]\left[1 + \frac{2\pi n_0}{\alpha}\right] \\
&\leq \left[2\alpha F(\frac{n}{\alpha}) + F(n)\right][1 + 2\pi 1] \qquad \textit{(Since } \frac{n_0}{\alpha} < 1 \textit{ by case assumption)} \\
&\leq \left[2\alpha\epsilon\frac{n}{\alpha} + F(n)\right][1 + 2\pi] \qquad \textit{(Since } \frac{n}{\alpha} \geq n_0 \implies F(\frac{n}{\alpha}) \leq \epsilon\frac{n}{\alpha}\textit{)} \\
&\leq \left[2\alpha\epsilon\frac{n}{\alpha} + \epsilon n\right][1 + 2\pi] \qquad \textit{(Since } n \geq n_0 \implies F(n) \leq \epsilon n\textit{)} \\
&\leq [3\epsilon n][1 + 2\pi] \\
&= [\epsilon n][3 + 6\pi] \\
&\leq 22\epsilon n \qquad\qquad \textit{(Since } 3 + 6\pi \leq 22\textit{)}
\end{aligned}$$

Thus, in either case, for arbitrary $\epsilon > 0$, $|q(z)| \leq 22\epsilon n$. So $|q(z)| = o(n)$.

B Appendix: Dirichlet's Approximation Theorem

Dirichlet's Approximation Theorem says we have lots of ways to use rationals to efficiently approximate irrationals. In particular, if you're trying to approximate any $r \in \mathbb{R}$, then you can get arbitrarily close to it ($\frac{1}{N+1}$ for any $N \in \mathbb{N}$...kind of) by using a rational approximation involving a particular $\alpha \in \{1, \ldots, n\}$ and particular $p \in \mathbb{Z}$. That is:

$$\forall r \in \mathbb{R}, \forall N \in \mathbb{N}, \exists \alpha \in [n], \exists p \in \mathbb{Z} \text{ s.t.}$$
$$\left| r - \frac{p}{\alpha} \right| \leq \frac{1}{\alpha(N+1)}$$

We can naturally extend this to saying we have lots of ways to use roots of unity to efficiently approximate non-roots of unity, because:

- $e^{2\pi i \cdot rational}$ is a root of unity
- $e^{2\pi i \cdot irrational}$ is not a root of unity

In our particular application to Roth's theorem, we want to show that given a fixed $z = e^{i\theta}$ on the unit circle, we can always find a root of unity ω (s.t. $\omega^\alpha = 1$ and $\alpha \leq N$) that is close to it. So, in this case, the rational we want to approximate is the normalized argument of z: $r = \frac{\theta}{2\pi}$. So we have:

$$\exists \alpha \in [n], \exists p \in \mathbb{Z} \text{ s.t.}$$
$$\left| \frac{\theta}{2\pi} - \frac{p}{\alpha} \right| \leq \frac{1}{\alpha(N+1)}$$

Multiplyng both sides by 2π, we have

$$\exists \alpha \in [n], \exists p \in \mathbb{Z} \text{ s.t.}$$
$$\left| \theta - \frac{2\pi p}{\alpha} \right| \leq \frac{2\pi}{\alpha(N+1)}$$

What this is telling us is that for any fixed point on the unit circle with angle θ, there is always going to be a point with angle $\frac{2\pi p}{\alpha}$ that is close to it (in particular, within $\frac{2\pi}{\alpha(N+1)}$ of it). And that close point, that is $\omega = e^{\frac{2\pi p}{\alpha} i}$, is indeed a root of unity satisfying $\omega^\alpha = 1$ and $\alpha \leq N$.

We are almost done: we have that

$$|\arg z - \arg \omega| \leq \frac{2\pi}{\alpha(N+1)}$$

.

But we want a bound of the form:

$$|z - \omega| \leq ?$$

.

Question 15. *If we know the angle between two points z and ω on the unit circle, how can we tell how far apart they are?*

Answer 15. *Draw a diagram bisecting the angle between the two points. You will find that if we know $\beta = |\arg z - \arg \omega|$, then $|z - \omega| = 2 \sin \frac{\beta}{2}$.*

So, we know

$$|z - \omega| \leq 2 \sin \frac{\pi}{\alpha(N+1)}$$

And since $\sin x \leq x$ for positive x:

$$|z - \omega| \leq \frac{2\pi}{\alpha(N+1)}$$

So this tells us that, just like we needed, given any fixed point z on the unit circle, we never have to travel farther than $\frac{2\pi}{\alpha(N+1)}$ to find a root of unity ω close to it satisfying $\omega^\alpha = 1$ and $\alpha \leq N$.

It's satisfying to see how nicely this bound covers the unit circle. For example, choose $N = 3$ and see how far we have to travel from each of the four relevant roots of unity...