MATH 1D, WEEK 7 – ROOTS OF UNITY, AND THE FIBONACCI SEQUENCE

INSTRUCTOR: PADRAIC BARTLETT

Abstract. These are the lecture notes from week 7 of Ma1d, the Caltech mathematics course on sequences and series.

1. HW 4 information

- Homework average: 80%.
- Issues: people kinda messed up the Taylor series question somewhat, and were a little sloppy with their statements. I mostly chalked this up to midterms and mid-quarter fatigue; however, if you're concerned, check out the solutions online (or drop by during office hours, or shoot me an email.)

2. Roots of Unity

In the real numbers, the equation

$$x^n - 1 = 0$$

had only the solutions $\{1\}$, if n was odd, and $\{1, -1\}$ if n was even; a quick way to see this is simply by graphing the function $x^n - 1$ and counting its intersections with the x-axis.

In the complex plane, however, the situation is much richer; in fact, by the fundamental theorem of algebra, we know that the equation

$$z^n - 1 = 0$$

must have n solutions. A natural question to ask, then, is: What are they?

If we express z in polar coördinates as $re^{i\theta}$, we can see two quick things:

- $r = 1$. This is because $|r^n \cdot e^{in\theta}|$ is just r^n, and the only positive number r such that $r^n = 1$ is 1.
- $\theta = k\frac{2\pi}{n}$, for some k. To see this: simply use Euler's formula to write $e^{in\theta} = \cos(n\theta) + i\sin(n\theta)$. If this expression is equal to 1, we need to have $\cos(n\theta) = 1$ and $i\sin(n\theta) = 0$ (so that the imaginary and real parts line up!) – in other words, we need $n\theta$ to be a multiple of 2π.

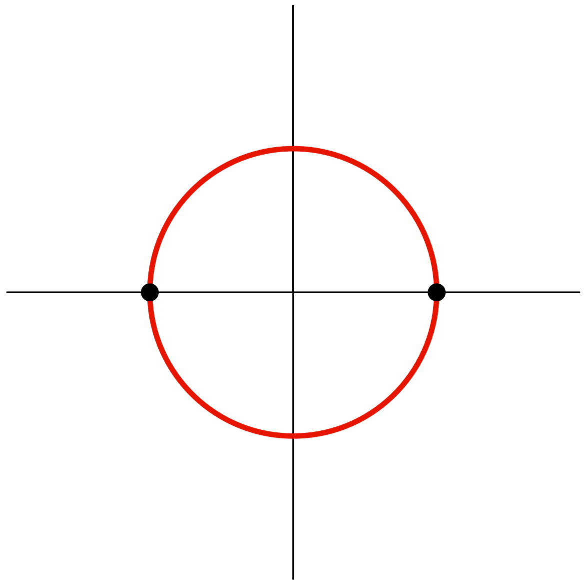
Combining these two results then tells us that the n distinct roots of $z^n - 1 = 0$ are

$$e^0, e^{\frac{2\pi}{n}}, e^{2\frac{2\pi}{n}}, e^{3\frac{2\pi}{n}} \ldots, e^{(n-1)\frac{2\pi}{n}}.$$

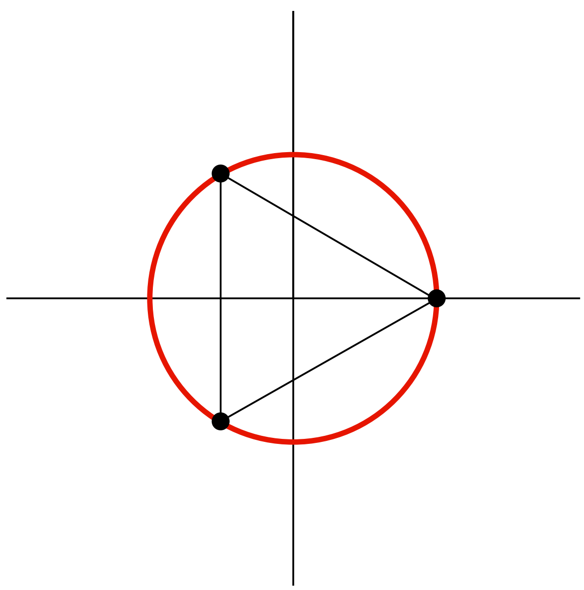
So: in some explicit cases, what are these roots?

Example 2.1. The only first root of unity is 1, as this is the unique solution to the equation $z - 1 = 0$.

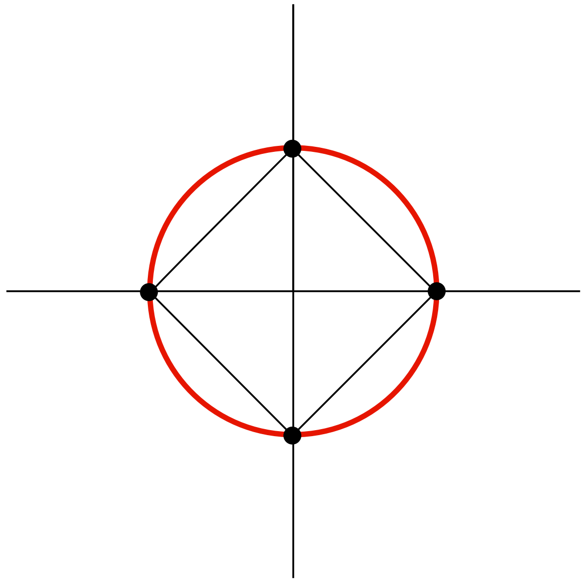
Example 2.2. The second roots of unity are, by the above, $e^0 = 1$ and $e^{\frac{2\pi}{2}} = e^{\pi} = \cos(\pi) + i\sin(\pi) = -1$, and can be graphed on the unit circle $|z| = 1$ as shown below:



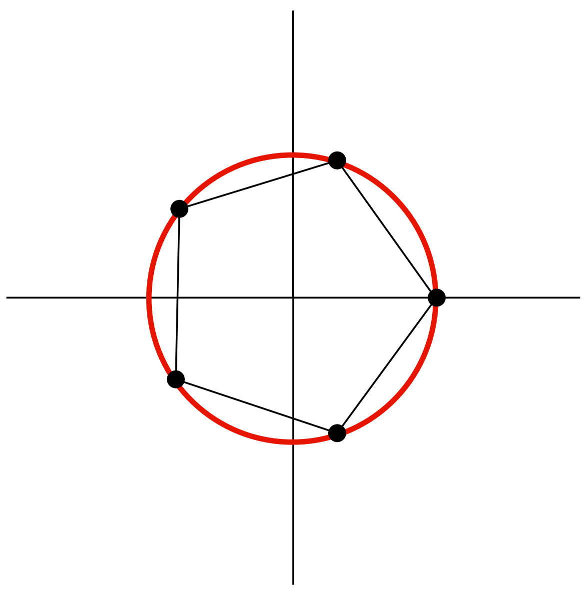
Example 2.3. The third roots of unity are simply (by the above) the points $e^0, e^{\frac{2\pi}{3}}$,, and $e^{\frac{4\pi}{3}}$; their graph is the three-equally-spaced points on the unit circle shown below.



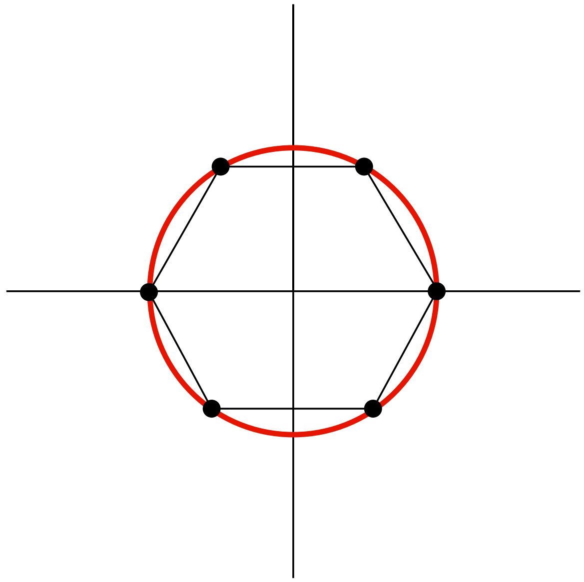
Example 2.4. The fourth roots of unity are the points $e^0, e^{\frac{2\pi}{4}}, e^{\frac{4\pi}{4}}$, and $e^{\frac{6\pi}{4}}$; in other words, by applying Euler's equation, they are $1, -1, i$, and $-i$. Their graph is the square inscribed in the unit circle:



Example 2.5. The fifth roots of unity are the points $e^0, e^{\frac{2\pi}{5}}, e^{\frac{4\pi}{5}}, e^{\frac{6\pi}{5}}$, and $e^{\frac{8\pi}{5}}$; in other words, they're just the five points corresponding to a regular pentagon inscribed on the unit circle, with one vertex at 1.



Example 2.6. The sixth roots of unity are the points $e^0, e^{\frac{2\pi}{6}}, e^{\frac{4\pi}{6}}, e^{\frac{6\pi}{6}}, e^{\frac{8\pi}{6}}$ and $e^{\frac{10\pi}{6}}$, and form the hexagon inscribed in the unit circle displayed below:



In the above pictures, these n-th roots of unity always correspond to the vertices of a regular n-gon inscribed in the unit circle. As it turns out, this is always true: a quick proof of this statement is just noticing that

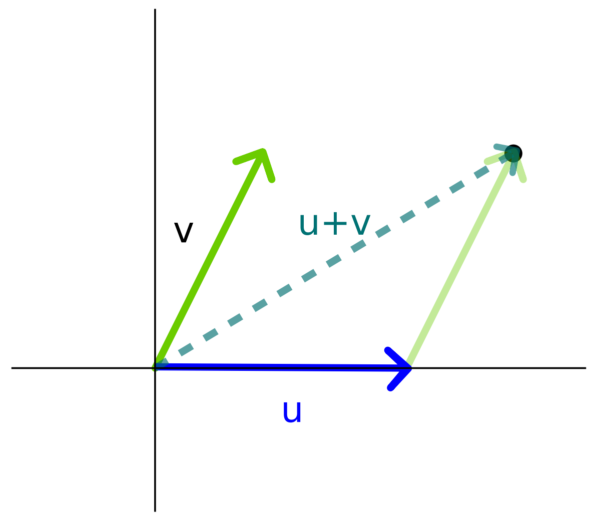
(1) we get all of our n-th roots of unity by starting at 1 and rotating by $\frac{2\pi}{n}$ around the unit circle, and
(2) doing this process creates n evenly-spaced points on the unit circle – i.e. the vertices of a n-gon.

The basic idea used above has a quick and remarkable consequence:

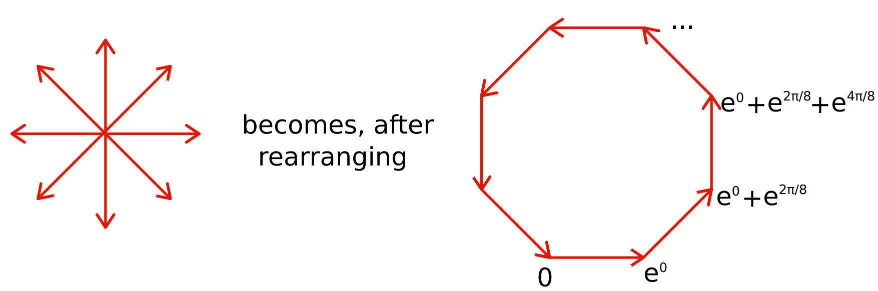
Theorem 2.7. *The sum of all of the n-th roots of unity is 0, for any $n \geq 2$.*

Proof. We start by stating something painfully trivial, but that visually is much less so:

Proposition 2.8. *The sum of any two points (a, b) and (c, d) in the plane is just $(a + c, b + d)$. In other words: if u and v are a pair of vectors based at the origin, then the vector $u + v$ can be acquired by placing the start of v at the tip of u, as shown below:*



Given this idea, we can visualize adding up the roots of unity in the following way: simply start with the vector made by the point e^0 and the origin, and add in sequence the vectors formed by the points $e^{k\frac{2\pi}{n}}$. As we discussed above, and is visually apparent in the picture below, these are all vectors of length 1 at angles $2\pi k/n$; so, adding them up visually creates a n-gon. But what does this mean about their sum? Well, that if we add all of these vectors together, we return to where we started. But the only number that has this property is 0 – so their sum is 0, as claimed.



□

The above is a rather unexpected property, and raises perhaps a parallel question: if their sum has such an odd property, what happens to their product? We answer this question with the following theorem:

Theorem 2.9. *The product of all of the n-th roots of unity is $(-1)^{n-1}$, for any n.*

Proof. So: first, begin by writing all of the n-th roots of unity in the form $\left(e^{\frac{2\pi}{n}}\right)^k$, where k can range from 0 to $n-1$. Then, we have that the product of all of the

n-th roots of unity is just

$$\begin{aligned}\prod_{k=0}^{n-1}\left(e^{\frac{2\pi}{n}}\right)^k &= \exp\left(\frac{2\pi}{n}\cdot\sum_{k=0}^{n-1}k\right)\\ &= \exp\left(\frac{2\pi}{n}\cdot\frac{n(n-1)}{2}\right)\\ &= e^{(n-1)\pi}\\ &= (-1)^{n-1},\end{aligned}$$

where the above steps were done by using the rules of multiplication and exponentiation, and Euler's summation formula. (for those of you who haven't seen it before: $\exp(x)$ is just the function e^x, and is used whenever actually writing a bunch of things in the exponent would render the mathematics unreadable.) □

3. Primitive Roots of Unity

At the start of our discussions, when we examined several concrete examples of roots of unity, we noticed that quite a few numbers were n-th roots of unity for several values of n. For example, amongst the sixth roots of unity $\{e^0, e^{\frac{2\pi}{6}}, e^{\frac{4\pi}{6}}, e^{\frac{6\pi}{6}}, e^{\frac{8\pi}{6}}, e^{\frac{10\pi}{6}}\}$, four of these values are in fact roots of unity for earlier values: in specific,

- $e^{4\pi/6}$ and $e^{8\pi/6}$ are both third roots of unity,
- $e^{6\pi/6}$ is a second root of unity, and
- e^0 is a root of unity for every n.

So, a natural question to ask here might be: "How many *new* roots of unity do we get for every n?" In other words: how many distinct values z are there such that

- $z^n = 1$, but
- $z^k \neq 1$, for all $1 \leq k \leq n-1$?

Such roots – the **primitive roots of unity** – have a host of interesting properties, which we will illuminate through a few questions.

The first thing we might ask is "How many primitive n-th roots of unity are there, for a given n?"

n	all n-th roots of unity	primitive n-th roots of unity
1	1	1
2	$1, -1$	-1
3	$1, e^{2\pi/3}, e^{4\pi/3}$	$e^{2\pi/3}, e^{4\pi/3}$
4	$1, e^{2\pi/4}, e^{4\pi/4}, e^{6\pi/4}$	$e^{2\pi/4}, e^{6\pi/4}$
5	$1, e^{2\pi/5}, e^{4\pi/5}, e^{6\pi/5}, e^{8\pi/5}$	$e^{2\pi/5}, e^{4\pi/5}, e^{6\pi/5}, e^{8\pi/5}$
6	$1, e^{2\pi/6}, e^{4\pi/6}, e^{6\pi/6}, e^{8\pi/6}, e^{10\pi/6}$	$e^{2\pi/6}, e^{8\pi/6}$
7	$1, e^{2\pi/7}, e^{4\pi/7}, e^{6\pi/7}, e^{8\pi/7}, e^{10\pi/7}, e^{12\pi/7}$	$e^{2\pi/7}, e^{4\pi/7}, e^{6\pi/7}, e^{8\pi/7}, e^{10\pi/7}, e^{12\pi/7}$
8	$1, e^{2\pi/8}, e^{4\pi/8}, e^{6\pi/8}, e^{8\pi/8}, e^{10\pi/8}, e^{12\pi/8}, e^{14\pi/8}$	$e^{2\pi/8}, e^{6\pi/8}, e^{10\pi/8}, e^{14\pi/8}$
9	$1, e^{2\pi/9}, e^{4\pi/9}, e^{6\pi/9}, e^{8\pi/9}, e^{10\pi/9}, e^{12\pi/9}, e^{14\pi/9}, e^{16\pi/9}$	$e^{2\pi/9}, e^{4\pi/9}, e^{8\pi/9}, e^{10\pi/9}, e^{14\pi/9}, e^{16\pi/9}$

We can find most small cases by hand; to generate the above table, for example, all we had to do to find the primitive n-th roots of unity is find all of the n-th roots of unity, and remove all of the ones that were k-th roots of unity for some smaller k. A pattern for the number of primitive roots might not be terribly obvious from the above, but a few quick conjectures can be made from the above data:

- Any prime number p has $p-1$ primitive roots of unity. This can actually be proven pretty quickly: if p is a prime number, then take any p-th root of unity $e^{2\pi k/p}$. Raising this quantity to some power m then yields the complex number $\left(e^{2\pi k/p}\right)^m = e^{2\pi km/p}$; in order for this to be equal to 1, we would have to have km/p be an integer. Because $k < p$, we know that $\text{GCD}(p, k) = 1$; so the only way in which km/p is an integer is if m is a multiple of p (and thus is bigger than p.)
- So: the only interesting thing in the proof above was that for km/p to be an integer, we had to have m be a multiple of p! This allows us to actually generalize our above conjecture massively:

  Theorem 3.1. *Any number n has $\phi(n)$-many primitive roots of unity, where $\phi(n)$ is the number of positive integers less than n that are coprime to n (i.e. their GCD with n is 1).*

  The proof of this is exactly the above: for any such number k coprime to n, the argument above tells us that $\left(e^{2k\pi/n}\right)^m$ is only 1 if m is a multiple of n. Conversely, if k is not coprime to n, we can let $m = n/\text{GCD}(n, k)$; this will always be an integer less than n such that $\left(e^{2k\pi/n}\right)^m = 1$.

So: perhaps motivated by our earlier discussions of sums and products, we can ask what the sums and products of all of the primitive n-th roots of unity are! Below is another table, summarizing the first few results that we can derive by hand:

n	sum of primitive n-th roots	product of n-th roots
1	1	1
2	$e^{2\pi/2} = -1$	$e^{2\pi/2} = h-1$
3	$e^{2\pi/3} + e^{4\pi/3} = -1$	$e^{2\pi/3} \cdot e^{4\pi/3} = e^{6\pi/3} = 1$
4	$e^{2\pi/4} + e^{6\pi/4} = 0$	$e^{2\pi/4} \cdot e^{6\pi/4} = e^{8\pi/4} = 1$
5	$e^{2\pi/5} + e^{4\pi/5} + e^{6\pi/5} + e^{8\pi/5} = -1$	$e^{2\pi/5} \cdot e^{4\pi/5} \cdot e^{6\pi/5} \cdot e^{8\pi/5} = e^{20\pi/5} = 1$
6	$e^{2\pi/6} + e^{8\pi/6} = 1$	$e^{2\pi/6} \cdot e^{8\pi/6} = e^{12\pi/6} = 1$
7	$e^{2\pi/7} + e^{4\pi/7} + \ldots + e^{12\pi/7} = -1$	$e^{2\pi/7} \cdot e^{4\pi/7} \cdot \ldots \cdot e^{12\pi/7} = e^{42\pi/7} = 1$
8	$e^{2\pi/8} + e^{6\pi/8} + e^{10\pi/8} + e^{14\pi/8} = 0$	$e^{2\pi/8} \cdot e^{6\pi/8} \cdot e^{10\pi/8} \cdot e^{14\pi/8} = e^{32\pi/8} = 1$
9	$e^{2\pi/9} + e^{4\pi/9} + \ldots + e^{16\pi/9} = 0$	$e^{2\pi/9} \cdot e^{4\pi/9} \cdot \ldots \cdot e^{16\pi/9} = e^{54\pi/9} = 1$
10	$e^{2\pi/10} + e^{6\pi/10} + e^{14\pi/10} + e^{18\pi/10} = 1$	$e^{2\pi/10} \cdot e^{6\pi/10} \cdot e^{14\pi/10} \cdot e^{18\pi/10} = e^{40\pi/10} = 1$
11	$e^{2\pi/12} + e^{4\pi/11} + \ldots + e^{20\pi/11} = -1$	$e^{2\pi/12} \cdot e^{4\pi/11} \cdot \ldots \cdot e^{20\pi/11} = e^{110\pi/11} = 1$

A few words should be said about how we actually calculated these values. The products were fairly straightforward; we just multiplied, summed the exponents, and looked at the result. The sums, however, were more in-depth: by looking at the explicit values, for example, it's not obvious what something like $e^{2\pi/3} + e^{4\pi/3}$ is! However, we *do* know, from earlier, that $1 + e^{2\pi/3} + e^{4\pi/3} = 0$, as these are all of the 3rd roots of unity; so just adding up the primitive roots of unity $e^{2\pi/3} + e^{4\pi/3}$ must give us -1.

This method, in fact, generalizes rather nicely. So: first notice that we can write the sum of all of the n-th roots of unity as just the sum of all of the primitive d-th roots, for every d that divides n – i.e.

$$(\text{sum of all } n\text{th roots}) = \sum_{d \text{ divides } n} (\text{sum of all primitive } d\text{th roots}).$$

But the sum of all of the n-th roots is always 0,as we showed earlier: so, we can rearrange this equation to see that

$$(\text{sum of primitive } n\text{th roots}) = -1 \cdot \sum_{d \text{ divides } n, d<n} (\text{sum of all primitive } d\text{th roots}).$$

In other words, this tells us that we can get the sum of all of the primitive n-th roots by just adding up the sums of all of the primitive d-th roots, for all of the d's that are proper divisors of n, and multiplying all of that by -1. In practice, this tells us that we can find, say, the sum of 6's primitive roots of unity by adding together the previously-calculated quantities of the sums of the third, second, and first roots of unity ($-1 + -1 + 1 = -1$) and multiplying by -1. This gives that the sum of 6's roots of unity is 1; a similar method will work to find every other sum here. (Question: can you find a pattern here?)

As for products, the pattern is far clearer:

Theorem 3.2. *The product of all of the primitive n-th roots of unity is always 1, as long as $n \neq 2$.*

Proof. So; just like before, notice that we can write

$$(\text{product of all } n\text{th roots}) = \prod_{d \text{ divides } n} (\text{product of all primitive } d\text{th roots});$$

so, because this product is always $(-1)^n$, we have that

$$(\text{product of all primitive } n\text{th roots}) = (-1)^{n-1} \prod_{d \text{ divides } n, d<n} (\text{product of all primitive } d\text{th roots}).$$

So: we consider two cases.

(1) If n is odd, then $(-1)^{n-1}$ is always 1; so we have that for every odd prime p,

$$(\text{product of all primitive } p\text{th roots}) = 1 \cdot 1 = 1.$$

By inducting on the number of odd factors of n, this tells us that the product of all primitive n-th roots is always 1, for any odd n.

(2) If n is even, then $(-1)^{n-1}$ is always -1; so we have that for every odd prime p,

$$(\text{product of all primitive } 2p\text{-th roots}) = (-1) \cdot (-1) = 1,$$

because the product of all primitive second roots of unity is -1, and this is the only number dividing $2p$ that's not p (which, as noted above, has the product of its primitive roots equal to 1 for any odd prime.) As well – by direct calculation – we can see that this property holds if p is the sole even prime 2, as the product of all primitive fourth roots of unity is 1.

Then, just as before, inducting on the number of factors of n tells us that the product of all primitive n-th roots is always 1, for any even n greater than 2.

So we're done! $\square$