2/20/15

HW 3 due Fri Feb 27
Spring Break Mar 9 – 13.
I'm out of town Mon Mar 16.

Where were we?

We had just proved de Moivre's Theorem:

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

Proof: Recall that each $z \in \mathbb{C}$ corresponds to a linear function

$$f_z : \mathbb{R}^2 \to \mathbb{R}^2.$$

In particular, we showed that the function $f_{\cos\theta + i\sin\theta} : \mathbb{R}^2 \to \mathbb{R}^2$ is just rotation c.c.w. by angle θ. It follows that

$$f_{(\cos\theta+i\sin\theta)^n} = \left(f_{\cos\theta+i\sin\theta}\right)^n \quad [\text{Why?}]$$

$$= f_{\cos(n\theta)+i\sin(n\theta)}. \quad [\text{Why?}]$$

Since these two functions are equal,

⇓

We conclude [why?] that

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

///

I really hate writing all that, so let's invent a temporary notation. Let

$$\text{cis}(\theta) := \cos\theta + i\sin\theta.$$

Then de Moivre's Theorem says

$$\text{cis}(\theta)^n = \text{cis}(n\cdot\theta).$$

But more is true.

Theorem: For all angles α, β we have

$$\text{cis}(\alpha+\beta) = \text{cis}(\alpha)\cdot\text{cis}(\beta).$$

Proof: This is equivalent to the statement that "rotation by β c.c.w. followed by rotation by α c.c.w. is the same as rotation by $\alpha+\beta$ c.c.w."

$\blacksquare$

Writing this out explicitly gives

$$\cos(\alpha+\beta) + i\sin(\alpha+\beta)$$

$$= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)$$

$$= \cos\alpha\cos\beta + i\sin\alpha\sin\alpha + i\cos\alpha\sin\beta + \underbrace{i^2}_{-1}\sin\alpha\sin\beta$$

$$= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta).$$

Comparing <u>real</u> and <u>imaginary</u> parts gives

$$\begin{cases} \cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta \\ \sin(\alpha+\beta) = \cos\alpha\sin\beta + \sin\alpha\cos\beta \end{cases}.$$

"Angle-Sum Formulas".

You never have to remember these.
Just remember

$$\text{cis}(\alpha+\beta) = \text{cis}(\alpha)\,\text{cis}(\beta).$$

"rotation by $\alpha+\beta$ = rotation by β, then by α"

Q: What other functions do you know with the property

$$f(\alpha + \beta) = f(\alpha) f(\beta) \quad \forall \alpha, \beta \quad ?$$

A: There is only <u>one</u> kind of function like this:

$$f(t) = e^{kt}$$

for some constant k.

This suggests that $cis(t) = e^{kt}$ for some k. <u>which</u> k?

Easy: Differentiate and then set $t = 0$.

$$e^{kt} = \cos t + i \sin t$$

$$k e^{kt} = -\sin t + i \cos t$$

$$k \underbrace{e^0}_{1} = -\underbrace{\sin 0}_{0} + i \underbrace{\cos 0}_{1}$$

$$k = i.$$

We have just proved

☆ Theorem (Euler's Formula, 1748)

$$\boxed{e^{it} = \cos t + i \sin t}$$

People like this formula because it looks kind of mysterious:

$$\text{"} e^{i\pi} = -1 \text{"}$$

But it is mostly a convenient notation. We can now drop the "cis":

$$\text{cis}(\theta) = e^{i\theta}.$$

So what? This is the last piece we need to really understand the field of complex numbers.

Recall that we can view complex numbers as vectors in the plane:

$$\text{"} a + ib \text{"} = (a, b).$$

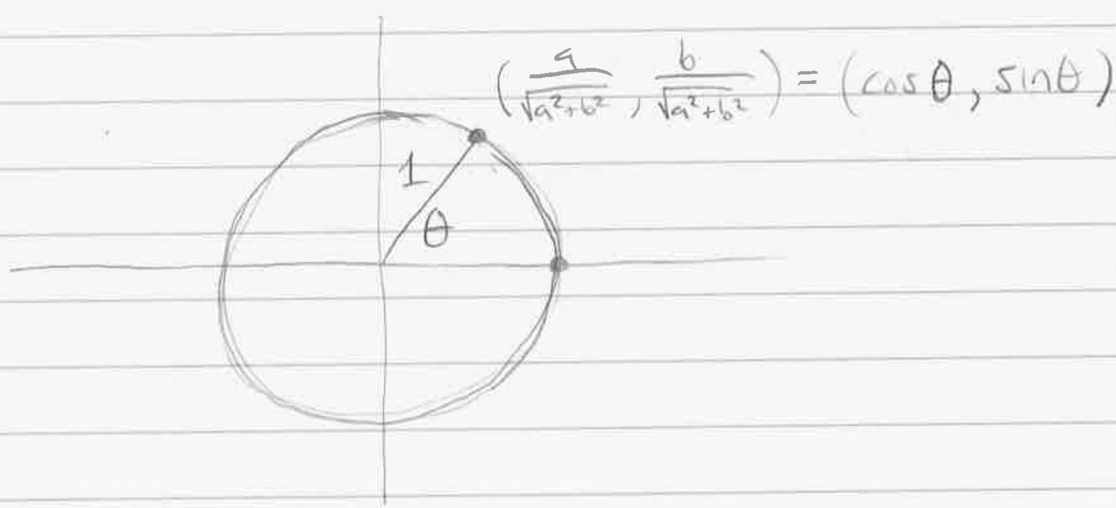
Addition is vector addition, but what is multiplication?

$uv = \text{what?}$

The answer is to express $u, v \in \mathbb{C}$ in "polar form".

$$u = a + ib = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}}\right).$$

Note that $\left(a/\sqrt{a^2+b^2},\ b/\sqrt{a^2+b^2}\right)$ is on the unit circle, so it must have the form $(\cos\theta, \sin\theta)$ for some angle θ.



We conclude that

$$u = |u|(\cos\theta + i\sin\theta) = |u|e^{i\theta}.$$

Suppose that complex number $v \in \mathbb{C}$ has angle φ measured c.c.w. from real axis, so

$$v = |v|e^{i\varphi}.$$

Then the product is

$$\begin{aligned} uv &= |u|e^{i\theta}|v|e^{i\varphi} \\ &= |u||v|e^{i\theta}e^{i\varphi} \\ &= |uv|e^{i\theta + i\varphi} \\ &= |uv|e^{i(\theta+\varphi)}. \end{aligned}$$

Conclusion: To multiply complex numbers, we multiply the lengths & add the angles.

[This was first noticed by Caspar Wessel in 1797, almost 50 years after Euler's Formula!]

2/23/15

HW 3 due this Fri Feb 27

Math Club Today!

Exam 1 Stats:

Total = 25

Average = 18.3

Median = 18

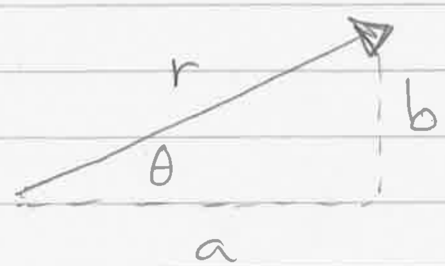
Approximate Grade Ranges:

21-25 ≈ A (13 students)

17-20 ≈ B (16 students)

10-16 ≈ C (11 students)

Recall: We can express complex numbers in either Cartesian or polar coordinates.



$$a + ib = r \cdot e^{i\theta}$$

Cartesian coordinates are good for addition:

$$(a+ib)+(c+id) = (a+c)+i(b+d)$$

Polar coordinates are good for multiplication:

$$(r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = (r_1 r_2)\, e^{i(\theta_1+\theta_2)}$$

"multiply the lengths & add the angles".

[This geometric interpretation of multiplication was first observed by Caspar Wessel in 1797, almost 50 (!) years after Euler's Formula.]

Finally we can return to the theme of this course: solving polynomial equations.

Until now we could only solve equations of low degree. Now we can solve equations of arbitrary degree (as long as they only involve multiplication).

Example: Solve $x^3 - 1 = 0$.

In other words, solve $x^3 = 1$. We are looking for the cube roots of 1. By Descartes' Theorem there can be at most 3 solutions.

We will look for complex solutions. Let

$$x = r e^{i\varphi}$$

where $r, \theta \in \mathbb{R}$. We will also express 1 in polar form:

$$1 = 1 \cdot e^{i0}$$

Then we have

$$x^3 = 1$$
$$(re^{i\varphi})^3 = 1e^{i0}$$
$$r^3 e^{i3\varphi} = 1e^{i0}.$$

Q: When are two complex numbers in polar form equal?

First, the lengths must be equal.
What about the angles?

Note that

$$e^{i\theta} = 1 \iff \theta = 2\pi k \text{ for some } k \in \mathbb{Z}.$$

Then we have

$$e^{i\varphi} = e^{i\mu} \iff e^{i\varphi}/e^{i\mu} = 1$$

$$\iff e^{i\varphi - i\mu} = 1$$

$$\iff e^{i(\varphi - \mu)} = 1$$

$$\iff \varphi - \mu = 2\pi k, \ k \in \mathbb{Z}.$$

///

Returning to $x^3 = 1$, we have

$$r^3 e^{i3\theta} = 1 e^{i0}$$

$$\Longrightarrow \begin{cases} r^3 = 1 \\ 3\theta = 2\pi k \text{ for some } k \in \mathbb{Z}. \end{cases}$$

$$\Longrightarrow \begin{cases} r = 1 \\ \theta = 2\pi k/3, \quad k \in \mathbb{Z}. \end{cases}$$

We obtain the solutions

$$x = e^{i2\pi k/3}, \quad k \in \mathbb{Z}.$$

But this looks like ∞ many solutions!
We only want 3.

Note that

$$e^{i2\pi k/3} = e^{i2\pi l/3} \iff \frac{2\pi k}{3} - \frac{2\pi l}{3} \in 2\pi\mathbb{Z}.$$

$$\iff \frac{k}{3} - \frac{l}{3} \in \mathbb{Z}$$

$$\iff k - l \in 3\mathbb{Z}$$

i.e., there are really just 3 solutions

$$\cdots = e^{i2\pi(-3)/3} = e^{i0} = e^{i2\pi 3/3} = e^{i2\pi 6/3} = \cdots$$

$$\cdots = e^{i2\pi(-2)/3} = e^{i2\pi 1/3} = e^{i2\pi 4/3} = e^{i2\pi 7/3} = \cdots$$

$$\cdots = e^{i2\pi(-1)/3} = e^{i2\pi 2/3} = e^{i2\pi 5/3} = e^{i2\pi 8/3} = \cdots$$

We will choose a convenient representative from each of the 3 classes:

$$x = e^{i0}, \; e^{i2\pi/3}, \; e^{i4\pi/3}.$$

Explicitly,

$$x = \cos(0) + i\sin(0) = 1 + i \cdot 0$$

$$x = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$x = \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

We obtain

$$x^3 - 1 = (x-1)\left(x - \frac{1+i\sqrt{3}}{2}\right)\left(x - \frac{1-i\sqrt{3}}{2}\right),$$

which you already know from HW 1.

But now we have a general method to solve the equation $x^n - 1 = 0$.

↓

★ Solution of $x^n - 1 = 0$.

The solutions are called the "nth roots of unity (i.e., 1)" and they are given by

$$\sqrt[n]{1} = \{ e^{i2\pi k/n} : k = 0, 1, 2, \ldots, n-1 \}.$$

This allows us to factor $x^n - 1$ as

$$x^n - 1 = \prod_{k=0}^{n-1} \left(x - e^{i2\pi k/n} \right)$$

///

There is a nicer notation for this.

Define $\omega := e^{i2\pi/n}$, and call this a primitive nth root of unity. Then the set of nth roots is

$$1 = \omega^0, \omega, \omega^2, \omega^3, \ldots, \omega^{n-1}.$$

So that

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2) \cdots (x-\omega^{n-1}).$$

2/25/15

HW 3 due this Friday.

Recall: Last time we found that

$$e^{i\varphi} = 1 \iff \varphi = 2\pi k \text{ for some } k \in \mathbb{Z}.$$

This implies that complex numbers $re^{i\varphi}$ and $se^{i\mu}$ in polar form are equal if and only if

$$r = s \ \& \ \varphi - \mu = 2\pi k \text{ for some } k \in \mathbb{Z}.$$

Then we used this to solve the equation

$$x^n - 1 = 0.$$

Let $x = re^{i\varphi}$ in polar form. Then

$$x^n = 1$$
$$(re^{i\varphi})^n = 1 \cdot e^{i0}$$
$$r^n e^{in\varphi} = 1 \cdot e^{i0}$$

$$\implies r^n = 1 \implies r = 1$$

AND

$$n\varphi - 0 = 2\pi k$$

$$\varphi = 2\pi k/n \quad \text{for some } k \in \mathbb{Z}.$$

This gives us the general solution

$$x = e^{i2\pi k/n}, \quad k \in \mathbb{Z}.$$

But how <u>many</u> numbers does this represent? We know that the polynomial $x^n - 1$ (of degree n) can have at most n roots.

Notation: Given a number α we define

$$\alpha\mathbb{Z} := \{\alpha n : n \in \mathbb{Z}\}.$$

Then we have

$$e^{i2\pi k/n} = e^{i2\pi l/n} \iff \frac{2\pi k}{n} - \frac{2\pi l}{n} \in 2\pi\mathbb{Z}$$

$$\iff \frac{k}{n} - \frac{l}{n} \in \mathbb{Z}$$

$$\iff k - l \in n\mathbb{Z}.$$

So? You will show on HW4 (Later) that this defines an equivalence relation on the set $\mathbb{Z}$:

$$k \sim l \iff k - l \in n\mathbb{Z}.$$

This equivalence relation partitions the set $\mathbb{Z}$ into n disjoint classes

$$\begin{aligned}\mathbb{Z} = &\{\ldots, -2n, -n, 0, n, 2n, \ldots\} \\ \cup &\{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, \ldots\} \\ \cup &\{\ldots, 2-2n, 2-n, 2, 2+n, 2+2n, \ldots\} \\ &\vdots \\ \cup &\{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}\end{aligned}$$

To describe the solution to $x^n - 1 = 0$ we must choose one representative from each class. The choice is arbitrary, so we usually choose representatives

$$0, 1, 2, 3, \ldots, n-1$$

Finally, we have

↓

☆ Theorem (Roots of Unity):

Let n be a non-negative integer. The equation $x^n - 1 = 0$ has complete solution

$$x = e^0, e^{i2\pi/n}, e^{i2\pi 2/n}, \ldots, e^{i2\pi(n-1)/n}.$$

$$x \in \{ e^{i2\pi k/n} : k = 0, 1, 2, \ldots, n-1 \}.$$

These solutions are called the "n^{th} roots of unity". ///

Often people define $\omega := e^{i2\pi/n}$ so that

$$e^{i2\pi k/n} = (e^{i2\pi/n})^k = \omega^k.$$

Then the n^{th} roots of unity are

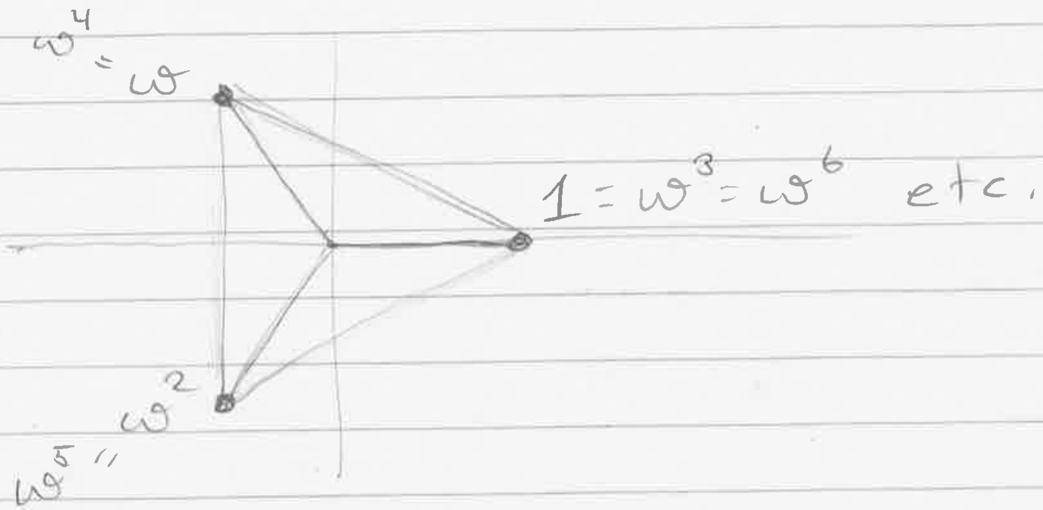
$$1, \omega, \omega^2, \omega^3, \ldots, \omega^{n-1}.$$

These are not so mysterious. Actually, they're just the vertices of a regular n-gon in the complex plane.

Example: Let $n = 3$. Then

$$\omega = e^{i2\pi/3} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$$

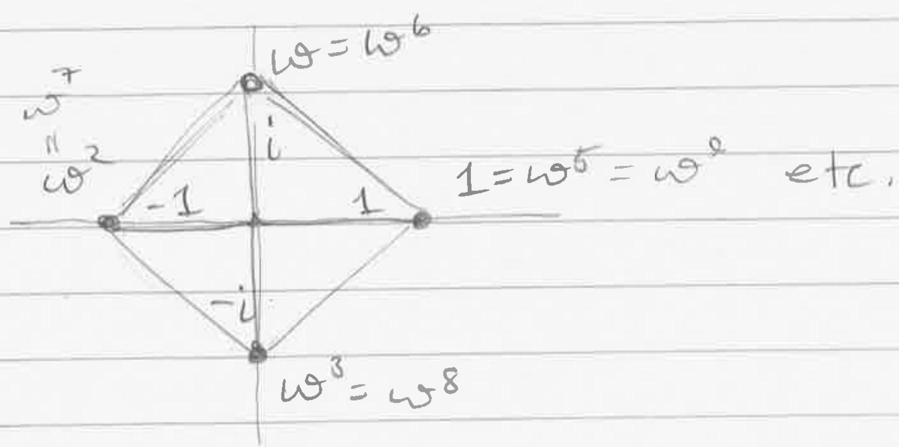
The 3^{rd} roots of unity are



Example: Let $n=4$ then

$$\omega = e^{i2\pi/4} = e^{i\pi/2} = i.$$

The 4^{th} roots of unity are



Q: Where is the center of the n-gon?

A: Obviously, the origin.

Q: Can you prove it?

The "center of mass" is

$$(1+\omega+\omega^2+\cdots+\omega^{n-1})/n.$$

We need to prove that this $= 0$.

Proof: Check that x^n-1 can be factored as

$$(x^n-1)=(x-1)(1+x+x^2+\cdots+x^{n-1})$$

Evaluate at ω to get

$$0=(\omega-1)(1+\omega+\omega^2+\cdots+\omega^{n-1}).$$

Since $\omega-1\neq 0$ we conclude that

$$1+\omega+\omega^2+\cdots+\omega^{n-1}=0.$$

///

This has an interesting consequence.
Recall that

$$\omega^k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right).$$

Our result says:

$$\sum_{k=0}^{n-1}\left(\cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)\right) = 0 + i0$$

$$\sum_k \cos\left(\frac{2\pi k}{n}\right) + i\sum_k \sin\left(\frac{2\pi k}{n}\right) = 0 + i0.$$

Comparing real and imaginary parts gives:

$$\begin{cases} \displaystyle\sum_{k=0}^{n-1} \cos\left(\frac{2\pi k}{n}\right) = 0 \\ \displaystyle\sum_{k=0}^{n-1} \sin\left(\frac{2\pi k}{n}\right) = 0 \end{cases}$$

[Could you prove these "real" identities without "imaginary" numbers? Probably not. Recall the Hadamard quote.]

2/27/15

HW 3 is due NOW.
HW 4 TBA
Spring Break Mar 9 — 13.
Exam 2 is Wed March 25.

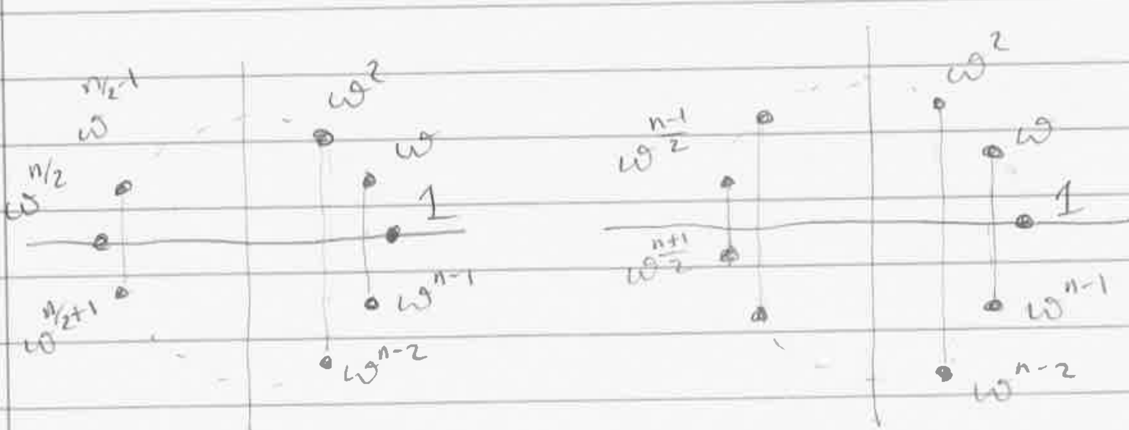
Last time we talked about

"Roots of Unity".

If we define $\omega := e^{2\pi i/n}$, then the n^{th} roots of 1 are given by

$$\sqrt[n]{1} = \{1, \omega, \omega^2, \omega^3, \ldots, \omega^{n-1}\},$$

and these are the vertices of a regular n-gon in the complex plane centered at the origin:



n even   n odd

Discussion:

- We can also take negative powers of ω. Given a positive integer k we define

$$\omega^{-k} := (\omega^{-1})^k = \frac{1}{\omega^k}$$

It has the formula

$$\omega^{-k} = e^{-2\pi i k/n}$$

This is also the complex conjugate of ω^k:

$$\omega^{-k} = \cos\left(-\frac{2\pi k}{n}\right) + i \sin\left(-\frac{2\pi k}{n}\right)$$

$$= \cos\left(\frac{2\pi k}{n}\right) - i \sin\left(\frac{2\pi k}{n}\right)$$

$$= (\omega^k)^*.$$

Since $\omega^n = 1$ we have

$$(\omega^k)^* = \omega^{-k} = \omega^n \cdot \omega^{-k} = \omega^{n-k},$$

as seen in the pictures above.

This is no surprise. HW 3(b) says that the complex roots of the real polynomial

$$x^n - 1$$

must come in conjugate pairs.

- Since we know the roots of $x^n - 1$, we can factor it as follows:

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

Then we can collect the factors into conjugate pairs of the form

$$(x-\omega^k)(x-\omega^{n-k}) = (x-\omega^k)(x-\omega^{-k})$$

$$= x^2 - (\omega^k + \omega^{-k})x + \omega^k\omega^{-k}.$$

But $\omega^k \omega^{-k} = \omega^0 = 1$, and

$$\omega^k + \omega^{-k} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$$

$$+ \cos\left(\frac{2\pi k}{n}\right) - i\sin\left(\frac{2\pi k}{n}\right)$$

$$= 2\cos\left(\frac{2\pi k}{n}\right).$$

Hence

$$(x-\omega^k)(x-\omega^{-k}) = \left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right)x + 1\right)$$

This allows us to completely factor $x^n - 1$ over the real numbers:

If n is even then

$$x^n - 1 = (x-1)(x+1)\prod_{k=1}^{\frac{n}{2}-1}(x-\omega^k)(x-\omega^{-k})$$

$$= (x-1)(x+1)\prod_{k=1}^{\frac{n}{2}-1}\left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right) + 1\right).$$

If n is odd then

$$x^n - 1 = (x-1)\prod_{k=1}^{\frac{n-1}{2}}(x-\omega^k)(x-\omega^{-k})$$

$$= (x-1)\prod_{k=1}^{\frac{n-1}{2}}\left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right)x + 1\right).$$

That's pretty cool, right?

• How much does $x^n - 1$ factor if we only allow rational (or integer) coefficients?

Well, we always have

$$x^n - 1 = (x-1)(1 + x + x^2 + \cdots + x^{n-1}).$$

Is it possible to factor

$$1 + x + x^2 + \cdots + x^{n-1} ?$$

Or is it "irreducible over $\mathbb{Z}$"?

Let's look at small examples:

$$x^2 - 1 = (x-1)(x+1)$$
$$x^3 - 1 = (x-1)(x^2 + x + 1)$$

The roots of $x^2 + x + 1$ are

$$x = \frac{-1 \pm \sqrt{-3}}{2},$$

which are <u>not</u> integers. ///

$$x^4 - 1 = (x-1)(x^3 + x^2 + x + 1)$$

Does $x^3 + x^2 + x + 1$ factor over $\mathbb{Z}$?

Since $x^4 - 1 = (x-1)(x+1)(x-i)(x+i)$ we know that

$$x^3 + x^2 + x + 1 = (x+1)(x-i)(x+i) = (x+1)(x^2+1).$$

$$\Longrightarrow x^4 - 1 = (x-1)(x+1)(x^2+1).$$ ///

Next, $x^5 - 1 = (x-1)\underbrace{(x^4 + x^3 + x^2 + x + 1)}_{\text{irreducible?}}$.

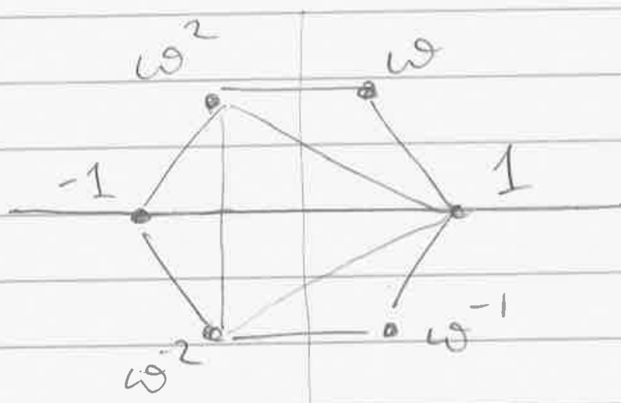
It turns out that $x^4 + x^3 + x^2 + x + 1$ <u>is</u> irreducible over $\mathbb{Z}$ but this is surprisingly difficult to prove. ///

Next, $x^6 - 1 = (x-1)\underbrace{(x^5 + x^4 + x^3 + x^2 + x + 1)}_{\text{irreducible?}}$

NO!

If $\omega = e^{2\pi i/6}$, then we know that

$$x^6 - 1 = (x-1)(x+1)(x-\omega)(x-\omega^{-1})(x-\omega^2)(x-\omega^{-2})$$



Note that $1, \omega^2, \omega^{-2}$ are the 3rd roots of unity, so that

$$x^3 - 1 = (x-1)(x-\omega^2)(x-\omega^{-2})$$
$$= (x-1)(x^2+x+1).$$

Note also that $\omega = -\omega^{-2}$, $\omega^{-1} = -\omega^2$ so that

$$(x-\omega)(x-\omega^{-1}) = (x+\omega^{-2})(x+\omega^2)$$
$$= ((-x)-\omega^{-2})((-x)-\omega^2)$$
$$= (-x)^2 + (-x) + 1$$
$$= x^2 - x + 1.$$

We conclude that

$$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1). \quad ///$$

Is there a pattern? Yes there is.

☆ **Theorem:** For each integer $k \geq 1$ there exists a polynomial $\Phi_k(x) \in \mathbb{Z}[x]$, irreducible over $\mathbb{Z}$, such that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

These $\Phi_k(x)$ are called the "cyclotomic polynomials"

Proof: This is too hard for MTH 461. ///

But the cyclotomic polynomials are not hard to compute. We've already seen several:

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = x^2 - x + 1$.

So, for example,

$$x^6 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)$$

because 1, 2, 3, 6 are the divisors of the number 6.

Thinking Problem:

Compute $\Phi_8(x)$.