Scene 1 and 2

In this video I'll try to show the solution of the problem of finding all n-th primitive roots of 1. First of all we'll briefly talk about complex numbers because the problem IS about complex numbers. So a little bit about what they are, how to denote, multiply them. Then, will talk about roots of complex numbers and how they differ from roots of real numbers. Next part will be about what is a group in abstract algebra and the generator of the group. After that we will combine these two, seemingly different topics and we will be almost at the end. So let's start.

Scene 3

The question has few layers to peel back in order to understand it, first we have to talk a little bit about complex numbers. They are more... complex than reals. It's the expansion of real numbers but not in a sense that real numbers were expansion of rationals numbers. We haven't found a place on a real axis between reals to place there complex numbers as we did with rational and real numbers. Instead of this, we add something like the second dimension. Real axis stays the same, it's the horizontal line, and we add vertical one and call it Imaginary. Now, we have a plane - complex plane.

We choose a point. Let's say that the first coordinate is a and the second one is b. We will denote our number z as $a + \imath b$, where $\imath$ is some special character, but we don't care about it now. $a + \imath b$ is called the algebraic form.

There's also another way of denoting our number. Instead of taking plane coordinates, we can consider the distance from the origin to the point and the angle between real positive half-axis and line going through our point and the origin. Using Pythagorean theorem we get the length, called modulus, and using some trigonometry, we get to know the angle. We will denote our number in a new form as $re^{i\varphi}$. It's called the 'exponential form'.

Scene 4

We call the plane on the right the polar plane. It's useful for visualization complex number multiplication. It's more convenient to see how it works on the polar plane. If we want to multiply two complex numbers written in the exponential form we multiply the modulus and add the angles. If we want to square our number we take the second power of modulus and multiply the angle by 2.

Scene 5

Now, we have to talk a little bit about roots of a complex number. The most important thing is that root is not a single number as it is with real numbers. The root is a solution to the equation $\varepsilon^n = z$, where ε is what we look for - the root.

ε_k - the way it looks

It happens that every ε being the solution can be written as follows: n-th root of r, the root is our well known root of a real number, times exponent of $\imath$ times φ plus $2k\pi$ over n, where k is an arbitrary integer. We can check that our ε is indeed the root by taking it to the $n-th$ power. We make some operations on exponents, take into account periodicity of the angle and we get it.

$k \in \mathbb{Z}_n$ explanation

Let $k = n + m$, such that m is smaller that n. Simplifying the expression shows that n does not influence the root. So instead of taking every integer, we can take k from the set from 0 to $n - 1$. We denote this set as $\mathbb{Z}_n$.

planes on the right

Looking at these roots we can observe some interesting properties. Roots lie on the circle with the center at the origin. Additionally, they are evenly distributed on the circle. That is to say the angle between two points is for given n always the same.

After showing polar planes with roots

Do you remember the task? „Find all primitive n-th roots of unity". Let's leave the word primitive for a moment. And we have „n-th roots of unity" and it simply means that our z is equal to 1. So, what does it mean in complex numbers? We are 1 unit form the origin, so r equals 1, and the angle is 0, so $\varphi = 0$. Our formulas are much more clear now. Entire set of the n-th roots of the unity is denoted as E_n.

Scene 6

We define a group as a set with some operation. Our group will be G with an operation 'asterisk'. We say that our pair is a group when it satisfies 4 requirements.

Group definition

The first requirement tells us that when we take 2 elements of G and combine them we will receive the element still belonging to G. So combining elements of G we will not get out of G.

The second one, we call it Associativity, tells us that it doesn't matter in what order we perform operations. By that I mean something really precise what's shown on the screen. We can't, for example, change the order of the elements in the equation but what we CAN change is the order of performing operations within this equation.

The third one is about the existence of a so called 'identity element' which doesn't change the element it is taking the operation with. We often sign it as 'e'. We call this element 'neutral element', too. By the way, there can only be one identity element in a group.

The fourth requirement tells us that for every element a in a group G, exists a special element such that when we combine them two we will get the neutral one. This special element is called the 'inverse' and for every a the inverse element is unique. We commonly denote it as a^{-1}, which is the inverse of a. Conversely, a is also the inverse of a^{-1}.

Integers group

One of the easiest groups is the integers with addition. Indeed, when we add two integers we get the integer. We know that it doesn't matter whether we add first and second integer and then the third one or add the second and third and this would be added to the first one. The neutral element is 0 and the inverse element to k is $-k$, because adding them both gives 0.

$\mathbb{Z}_n$ group

There's an interesting group - ($\mathbb{Z}_n$ set with addition modulo n). $\mathbb{Z}_n$ set is a set of integers from 0 to $n-1$. When we add modulo n two numbers it means first we add them and then get their remainder of division by n.

Let's look at the example - $\mathbb{Z}_8$. And add modulo 8 2 and 3. 2 plus 3 modulo 8 equals 5 modulo 8 equals 5. Now, 5 plus modulo 8 6. 5 plus 6 modulo 8 equals 11 modulo 8 equals 3 and so 3 is the answer.

Scene 7

We would like to define what does it mean to take the power of elements. We say that a^{k+1} is $a^k * a$, where k is the integer. a^0 is the group's neutral element. Now, when we have it, we can introduce generator's definition. We say a from group G is a generator of G if set of all integer powers of a is G. Using the generator we can generate entire group.

Integers group

Look at group Z with addition. Let $a = 2$. 2^0 is a neutral element so it is 0. Then using the definition we get that $2^1 = 2$, 2 squared is 4, 2 cubed is 6, 2^4 is 8. Now, negative powers, 2^{-1} is -2, because -2 + 2 is 0, using this scheme, we get -4, -6 and -8. Overall, 2 generates all even numbers, so it is not a generator of Z group. In general, a generates a group containing all integers divisible by a. So 1 generates entire Z group and IS the generator. Similarly, -1 is the generator of our Z group.

$\mathbb{Z}_n$ group

What about $\mathbb{Z}_n$ group? For example Z_8? 2 gives us a set of itself, 4, 6 and 0. 2 is not a generator of Z_8. Let's look at another example, 1. We get 1, 2, 3, 4, 5, 6, 7 and 8 or in other words, the entirety of Z_8. Therefore 1 is a generator of Z_8. Now, let's consider 3. We have 3, 6, 1, 4, 7, 2, 5 and 0, it means all numbers from 0 to 7, so 3 generates Z_8. As you can see there's no obvious answer to the question: what number is a generator.

Scene 8

You may wonder, why are we talking about such things and how do they relate to complex numbers? The answer is: E_n sets are groups with multiplication.

First of all, multiplication is an inner operation. When multiply two roots together, we will see that it works.

The second requirement was associativity. We write it down, use our knowledge about exponents, about Z group and go back, we get what we wanted.

The third one was the existence of neutral element. If we remember that 1 is always one of the roots of unity, we immediately know the neutral element because 1 multiplied by any number gives this number.

And the last one, inverse element. Multiplying ε_k and ε_l we get 1. It gives us that 2 times $k+l$ has to be 0, so $l = -k$, but l and k were the indexes of the roots and we do not have negative indexes. Thankfully, we can make a whole circle by adding n and we get, what we needed.

To sum up this part, we have already proven that E_n set with multiplication is a group.

By the way, entire set of complex numbers with addition is also a group and complex numbers without the number 0 this time with multiplication is a group, too.

Scene 9

Now, we are ready to fully understand the task. n-th roots of unity are complex roots of 1. Also, the word primitive stands for the generators of E_n group. So what we are looking for are elements of E_n which taken to the next powers successively give us entire E_n set. For now we know that not every element of a group is a generator. We will try to find out if there's any pattern to that.

Scene 10

Managing roots of 1 with all their quite complicated notation is annoying. Hopefully, having done some algebraic transformations, we will get something more inviting. We have a problem with $k+m$, but we know that in an exponent we care only about angles from 0 to 2π, so $k+m$ over n must be smaller than 1. We can get it by adding k and m modulo n. Thanks to this we see that multiplying elements of E_n is the same as adding their indexes modulo n. Such similarity is called isomorphism.

Now, we can look at the example. ε_2 cubed is in a sense the same as taking 2 to the power of 3 in $\mathbb{Z}_n$ group. ε_2 times ε_2 is ε_4 and ε_4 times ε_2 is ε_0. Likewise, 2 plus modulo 6 2 is 4 and 4 plus 4 modulo 6 is 0.

It means that we can consider our problem in terms of $\mathbb{Z}_n$ group instead of E_n group, which is much easier.

Scene 11

Ok, finally we should start solving the task. Let's assume n is greater or equal to 2. Case when $n = 1$ is boring, because E_n contains only 1. Now, we take k from $\mathbb{Z}_n$ and ask whether k is $\mathbb{Z}_n$'s generator.

This time, let's take m from $\mathbb{Z}_n$. Then raise k to the power of m, which translates to adding k to itself m times. Afterwards, calculate modulo n. In other words, it is k times m modulo n.

It's important to notice that after reaching 0 we will get nothing new. In the current example, right after arriving at 0 we will get 2 and that's what we started with. If we continue, we will again get 4, 0, 2, 4, 0 and so on. So what interests us is the first time we reach 0. This insight will be crucial to understand later parts of the reasoning.

But what does it mean that we reach 0? It means that k to the power of m can be written as n times some integer l nodulo n.

We would like to check something. Is it true that if the smallest power for which k hits 0 is strictly smaller than n then k does not generate $\mathbb{Z}_n$? Let's assume antecedent. It implies that number of elements of the generated group is smaller than number of elements in $\mathbb{Z}_n$ group. Therefore, generated group can not be $\mathbb{Z}_n$ and k is not a generator.

Let's try to write left-hand side more transparently. We have that k^b is $kb \mod n$ is 0.Equivalently saying, kb is a multiple of n. We denote it as $kb = ln$. It means that kb is divisible by n. And because none of k and b equal n, then n and k have greatest common divisor larger than 1. Now, it looks good enough.

We would like to have similar implication with a minor change: if gcd of n and k is 1 then k generates $\mathbb{Z}_n$. Let's use proof by contradiction.

So now, the implication changes to: if gcd of n and k is 1, then k does not generate $\mathbb{Z}_n$.

Let's develop some intuition. Assuming the implication was true, we would have two implications. The first one, the assumed one. And the second one, the already proven one, saying that if n and k have common divisor greater than 1 then k does not generate $\mathbb{Z}_n$. So, in both cases we are led to conclude that $\mathbb{Z}_n$ is not being generated by k. Equivalently, that there's no element being the generator. But, we have seen that they exist, before.

So, coming back to the proof. If gcd of n and k is 1 and k does not generate $\mathbb{Z}_n$, then there exists natural number a, smaller then n such that $ak = nl$ for some l. This means that ak is divisible by n and because n and k do not have any common divisors different to 1, n divides a. However, we have already assumed that a is strictly smaller than n, so n can not be its divisor. So we can conclude that our previous implication was true.

Scene 12

The final answer is: ε_k is a generator of E_n if and only if n and k are relatively prime.