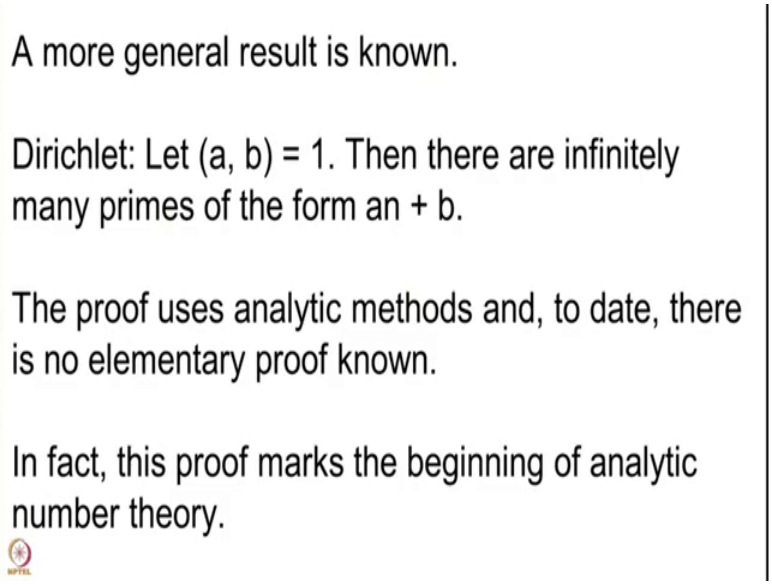
A Basic Course In Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 08
Winding up on Primes' and introducing Congruences'

Welcome back. We saw that there are infinitely many primes first of all, then there are infinitely many odd primes, then I told you prove that there are infinitely many prime which are of the form 4n plus 3 and I said in the end that there are indeed infinitely many primes of the form 4n plus 1, I indicated how that can be done but I did not complete one important step, I leaved that step to you.

I hope you will think about it and let me know your comments. You may ask is there a general result, why are we always looking at 2n plus 1 or 4n plus 1 or 4n plus 3, why cannot we do a more general thing?

(Refer Slide Time: 1:04)



A more general result is known.

Dirichlet: Let (a, b) = 1. Then there are infinitely many primes of the form an + b.

The proof uses analytic methods and, to date, there is no elementary proof known.

In fact, this proof marks the beginning of analytic number theory.

And indeed a more general result is known. This is due to Dirichlet which is proved more than a hundred years back, what does the result say? The result says the following, that we start with two natural numbers which are co-prime, which are relativity prime, their gcd is 1. If you start with a, comma b equal to 1, then there are infinitely many primes of the form an plus b.

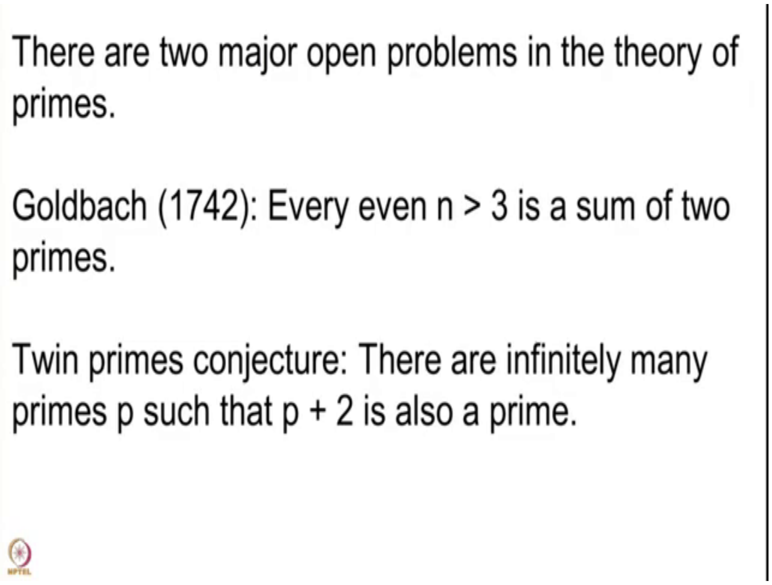
Note here that this condition that the gcd be equal to 1 is a necessary condition, for instance you may consider the set of the primes of the form 10n plus 5. If you put n equal to 0, you will get 5 but then for all other n, all other values of the natural numbers you will get numbers which are multiples of 5. So, if your gcd is not taken to be 1, there is no way that you are going to get infinitely many primes, you may at most get only one single prime, which is actually going to be the gcd.

So, the condition that ab, the gcd of a and b be equal to 1 is a necessary condition, it is important to be assume to have the result, but in this case as the theorem would tell you it is also sufficient, once you assume this then there are infinitely many primes in the set an plus b, how are the situated that is a different matter, right now we are only worrying about cardinality of the set of primes in the sequence in this arithmetic progression an plus b, this is the theorem of Dirichlet.

This proof uses analytic methods, this proof is before the proof of Hadamard and de la vallee Poussin of the prime number theorem, so it is indeed more than a hundred years back. And this prove is supposed to be the beginning of the branch of number theory which is called analytic number theory.

And to date there is no elementary proof known, for the prime number theorem we have an elementary proof, which is given by Selberg and Erdos and elementary just means that it does not use complex analysis, this proof uses analytic method and to date we do not know any proof which does not use analysis.

(Refer Slide Time: 4:11)



There are two major open problems in the theory of primes.

Goldbach (1742): Every even n > 3 is a sum of two primes.

Twin primes conjecture: There are infinitely many primes p such that p + 2 is also a prime.

Since, we are discussing about primes and we are almost coming to the end of our discussion on this theme or primes, let me also mention two very important open problems with the theory of primes. The first one is due to Goldbach, this is famous as Goldbach's conjecture, this was stated much before the legendary and Gauss's conjecture of the prime number theorem, this is in 1742, almost 300 years now more than 280 years.

And the theorem says that if you take any even integer n bigger than 3, then it is the sum of two primes, so very innocuous statement, actually number theory is famous for having statements which are very simple, the statement does not use any HiFi machinery, but the proofs are very difficult.

To date, we do not know any proof of this result, you can of course check this result in fact there are computers now which are very fast computers and people have used them to check that very big numbers, very big even numbers are sums of two primes that has been verified. Today there is not a single even number found which is not a sum of two primes, had such a number been found then we would have had a counter example and this statement would have been settled for once and all.

But we do not have a counter example and more importantly we do not also have a proof of this result. There is a result which is proved in this direction which says that if you relax the condition of having two primes, but say that one of them can be product of two primes then the result holds, what does it mean?

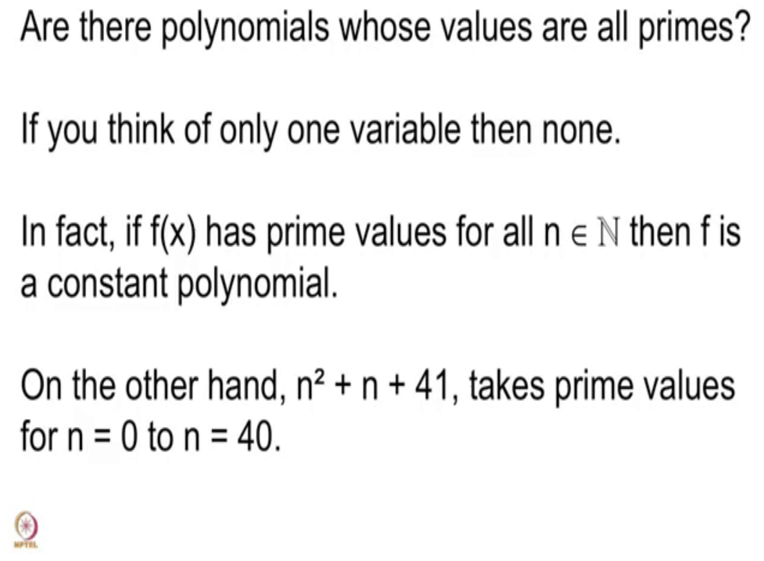
It means that given any n, any even n bigger than 3 we can write it as a plus b, where is a prime and b is product of at most two primes. This result is known that is already a difficult result but this result is known, so one can say that this is a positive step towards improving Goldbach's conjecture.

There is another conjecture which I have been talking about, this is the twin prime conjecture. The twin prime conjecture says that there are infinitely many primes p such that p plus 2 is also a prime. There is a lot of work done recently on this by Terence Tao and many other mathematicians.

The work talks about length between successive primes, so the problem here is to show that 2 occurs as length between two consecutive primes infinitely many times. This is also, there is sizable progress in this thing also and one would hope that these two results are proved, very soon these are two major open problems as far as theory of primes is considered.

In the number theory, even the elementary number theory there are many many open problems which are very difficult but we will not be discussing them right now, these two however are very major open problems.

(Refer Slide Time: 7:52)



Are there polynomials whose values are all primes?

If you think of only one variable then none.

In fact, if f(x) has prime values for all $n \in \mathbb{N}$ then f is a constant polynomial.

On the other hand, $n^2 + n + 41$, takes prime values for n = 0 to n = 40.

Now, this p and p plus 2 being a prime suggests that can we look at a polynomial whose values are all primes, can you have a polynomial? A polynomial is a function of the type f of x equal to a0 plus a1 x plus a2 x square plus dot dot dot upto an x power n, can you have a polynomial whose values are all primes?

All primes are given as the values of the polynomial, of course you can say that f of x equal to x is one such polynomial, but that is not what we want, what we want is whenever I put any value for x, the value that I get out of it whenever I put any n for the variable x the value that I get is always a prime that is what we are asking.

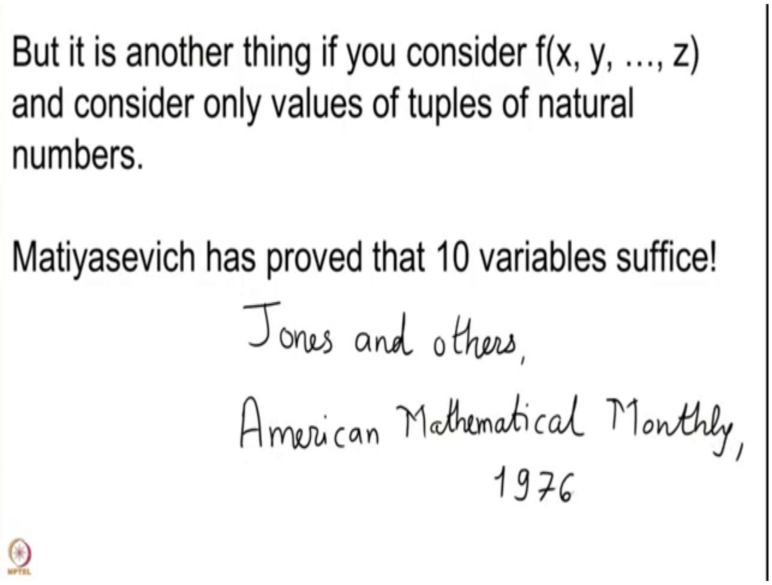
We can even relax the situation, we will say that we put only the natural numbers for x and then we should get primes, it is okay for negative integers we do not get primes, but for all natural numbers we should get primes, it is okay if we do not get all primes but for every natural number n fn should be a prime, is that possible? The answer is no, this is not possible.

And in fact, if f x has only prime values for all natural numbers n, then f is a constant polynomial, you can of course have the constant polynomial f of x equal to 5, this is going to give you the value 5 which is prime for every x, so f x equal to x is not allowed because for all natural numbers we do not get prime values, f x equal to constants are also not allowed because they are not interesting, we would like to get at least infinitely many values, distinct values. A constant polynomial will give you only one value.

So, if you are thinking about putting, having only one variable then the answer is no, but you can ask however let me also tell you that there are these interesting polynomials, there is this polynomial x square plus x plus 41, if you put natural numbers there, from n to 0 to all the way up to n equal to 40, all the values that we get are all primes, check it, take for any favorite number n from 0 to 40, put the value of n in this polynomial x square plus x plus 41 and check that you do get a prime quantity.

However, at 41 we do not get this, so that also gives us a very nice lesson that whenever you want to prove a result for all n or for infinitely many n it’s not good to check the result for some set of numbers, because you would have checked it for a set of numbers and you would think this should be true but then a counter example might be lurking at the very next step. So, now we change our questions slightly, we say that instead of polynomial in single variable we allow to increase the number of variables, do we now get a polynomial?

(Refer Slide Time: 11:20)



But it is another thing if you consider f(x, y, ..., z) and consider only values of tuples of natural numbers.

Matiyasevich has proved that 10 variables suffice!

Jones and others,

American Mathematical Monthly,

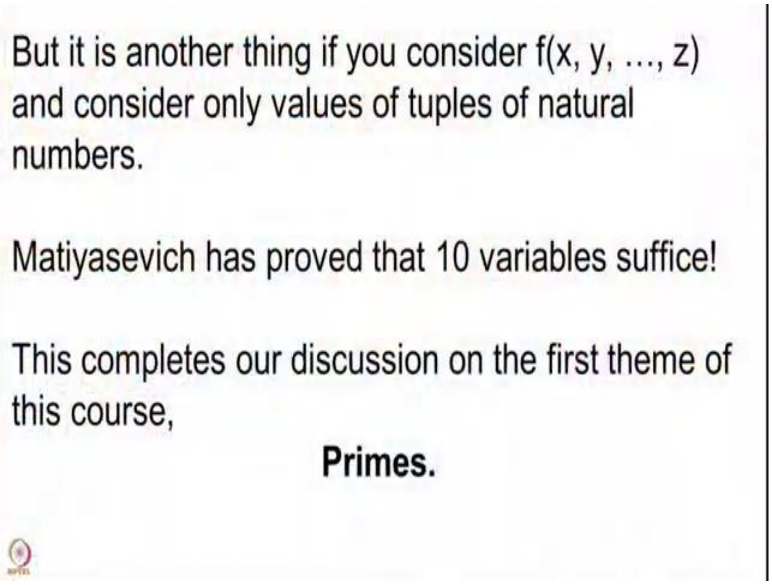
1976

So, it is another thing, remember what I said in the last slide that if you have only one variable then the answer is none, you cannot get any such non constant polynomial. So, you increase the number of variables, so your polynomial could be f of x, comma y, comma dot dot dot, comma z, we have increased the number of variables and we also agree that we will put for each of the variables only natural numbers.

So, if there are say k variables x1, x2, xk then we will consider f of n1, n2, nk, these are the only things that we are going to consider and then we are asking that this set should consist only of primes. The answer is yes, we do indeed have such a thing. In fact, Matiyasevich has proved that 10 variables suffice to prove, you can have 10 variables, you can have a polynomial f x1, x2, x3 up to x10, there is a polynomial that Matiyasevich writes.

And this polynomial is enough if you put natural numbers in it, all the values you get are all primes. And in fact, you get all primes as values. So, a good reference for this is the following paper of Jones and others. The journal is American Mathematical Monthly and you should look for an issue in 1976, you should search in Google for Jones American Mathematical Monthly 1976 and you will get a paper which discusses this, it lists, it writes down that polynomial in 10 variables, it also gives a proof of how by putting natural numbers in the variables in that polynomial in 10 variables we get all primes.

(Refer Slide Time: 14:02)



But it is another thing if you consider f(x, y, …, z) and consider only values of tuples of natural numbers.

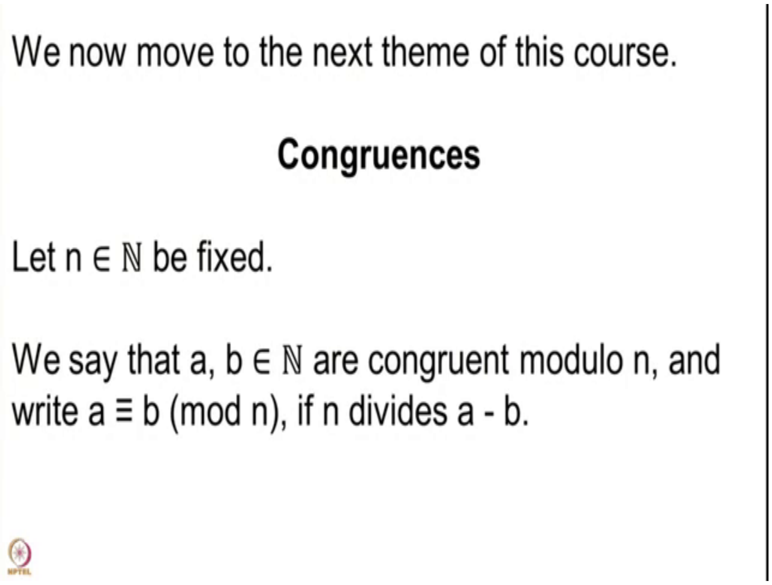
Matiyasevich has proved that 10 variables suffice!

This completes our discussion on the first theme of this course,

Primes.

With this we complete our discussion on the very first theme of our course. The very first theme of the course until now was primes, we have come to the end of this theme, we now begin our discussion on the second theme and so of course it does not mean that we will let the primes go but we will concentrate on some other properties of natural numbers.

(Refer Slide Time: 14:18)



We now move to the next theme of this course.

Congruences

Let $n \in \mathbb{N}$ be fixed.

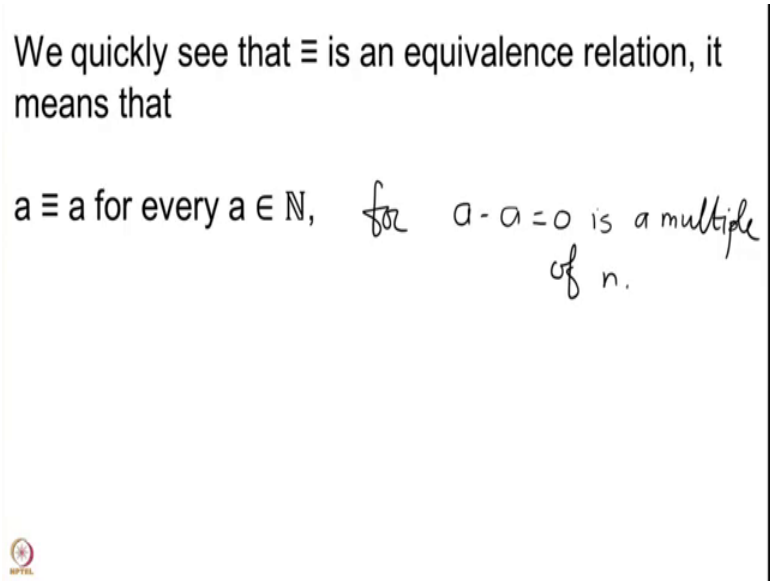
We say that $a, b \in \mathbb{N}$ are congruent modulo n, and write $a \equiv b \pmod{n}$, if n divides $a - b$.

So, we now move to the next theme of this course, this theme is called Congruences. This may be a word which you may not have seen if you have never had a course in Number Theory. It is a very simple notion actually. First, fix natural number n, so this number n will remain fixed for a length of our discussion and then having fixed this natural number n we take any two natural numbers a and b or you may take them even to be in z.

So, you take a, b and we say that they are congruent modulo n and this is written as a equal to b mod n, but that equality sign has one more horizontal line. So, that triple equality is what we call congruent. So, we will say that a is congruent to b modulo n if n divides the difference a minus b, so this is like imagine that you have a large disc and you are writing the numbers 1, 2, 3, 4, 5, 6, all the way up to n on that disk and you have a hand like minute hand or hour hand of hour clock which goes round and round, it will go to 1 then it goes to 2, then 3 and so on.

The moment it reaches n, next time it will go back to 1. So, n plus 1 is treated like 1 because the difference of n plus 1 and 1 is n, 2n plus 5 will be treated like 5 because the difference of 2n plus 5 and 5 is 2n which is multiple of n. So, you may think that congruence is nothing but imagining a clock where instead of 12 you have n digits that is how simple it is.

(Refer Slide Time: 16:45)



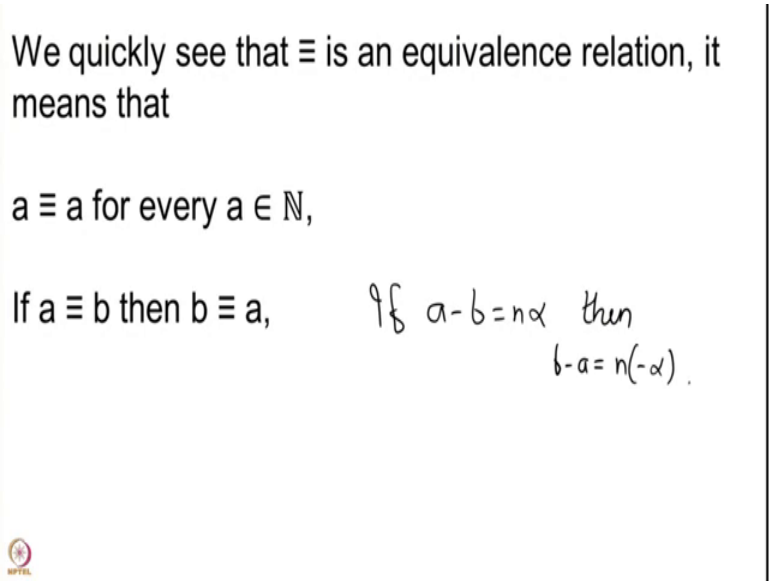
We quickly see that ≡ is an equivalence relation, it means that

$a \equiv a$ for every $a \in \mathbb{N}$, for $a - a = 0$ is a multiple of n.

This relation of congruence it is an equivalence relation. So, what does it mean to say that something is an equivalence relation? What is the relation first of all? Given any two integers we are talking about whether they are related by this congruence modulo n or not, that we are looking at.

So, further we say that this is an equivalence relation, meaning there are some important properties which are satisfied by this relation. What are those properties? Property number 1 is that for every a, a is congruent to a, but this is quite easy, you will have that a minus a which is 0 and a minus a being 0 is multiple of n, quite simple.

(Refer Slide Time: 18:02)



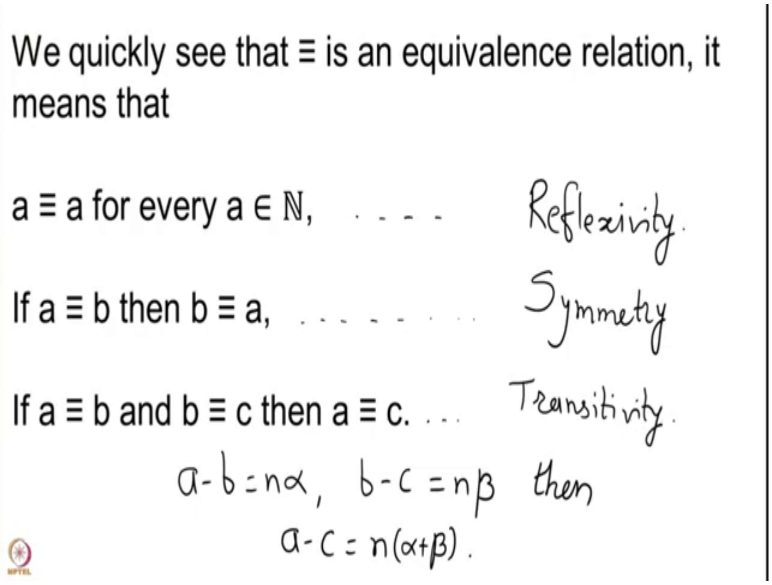
We quickly see that ≡ is an equivalence relation, it means that

$a \equiv a$ for every $a \in \mathbb{N}$,

If $a \equiv b$ then $b \equiv a$,   If $a-b=n\alpha$ then $b-a=n(-\alpha)$.

Then we have the next property which says that whenever a is congruent to b then b is congruent to a this is also quite simple because if a minus b is n times alpha then b minus a is and n times minus alpha so this is also. Whenever we have a congruent to b we will have that b is congruent to a. And finally the third property, the equivalence relation should satisfy three properties. First one, second one and now we go to the third one.

(Refer Slide Time: 18:43)



We quickly see that ≡ is an equivalence relation, it means that

$a \equiv a$ for every $a \in \mathbb{N}$, ... Reflexivity.

If $a \equiv b$ then $b \equiv a$, ... Symmetry

If $a \equiv b$ and $b \equiv c$ then $a \equiv c$. . . . Transitivity.

$a-b = n\alpha$, $b-c = n\beta$ then

$a-c = n(\alpha+\beta)$.

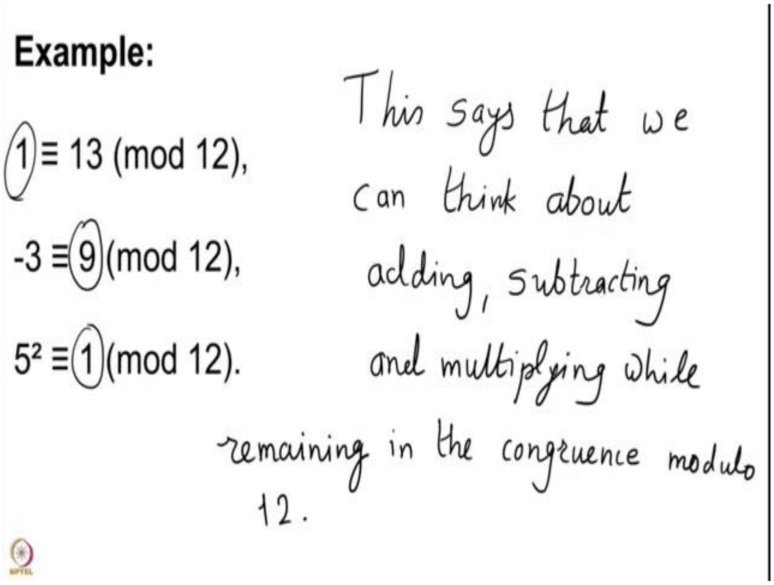
If a is congruent to b and b is congruent to c which might be yet another natural number, then a is congruent to c. So, we have that whenever a and b are related with respect to this equivalence relation b and c are related then a and c have to be related. This is also quite easy to see because if I have a minus b is n alpha, b minus c is n beta, we have that a minus c is going to be n times alpha plus beta.

So, all these three properties are very easy to prove and these three properties constitute an equivalence relation whenever such a thing holds we have an equivalence relation. I will not define the equivalence relation it is very much what I have written here but I will invite you to go and read some other source say ‘Wikipedia’ or some basic book on Number Theory to know more about equivalence relation.

But we will be using these properties quite often and these properties have their own name. So, this property is called reflexivity, whenever you have a relation which has the property that a is related to a for every a, then we say that the relation is reflective or that the relation satisfies reflexivity.

If a is congruent to b, then b is congruent to a, this relation is called symmetry, we will then say that the relation is symmetric whenever a is related to b, we have that b is related to a. And finally this third property is called transitivity or we will say that our relation is transitive. So, in short a relation is an equivalence relation if it is reflexive, symmetric and transitive and these things will be used later when we do more work with respect to the relation of congruence. For now let us go and see some examples. We are quite familiar with our usual clock so we are going to take n equal to 12.

(Refer Slide Time: 21:22)



Example:

$\textcircled{1} \equiv 13 \pmod{12}$,

$-3 \equiv \textcircled{9} \pmod{12}$,

$5^2 \equiv \textcircled{1} \pmod{12}$.

This says that we can think about adding, subtracting and multiplying while remaining in the congruence modulo 12.

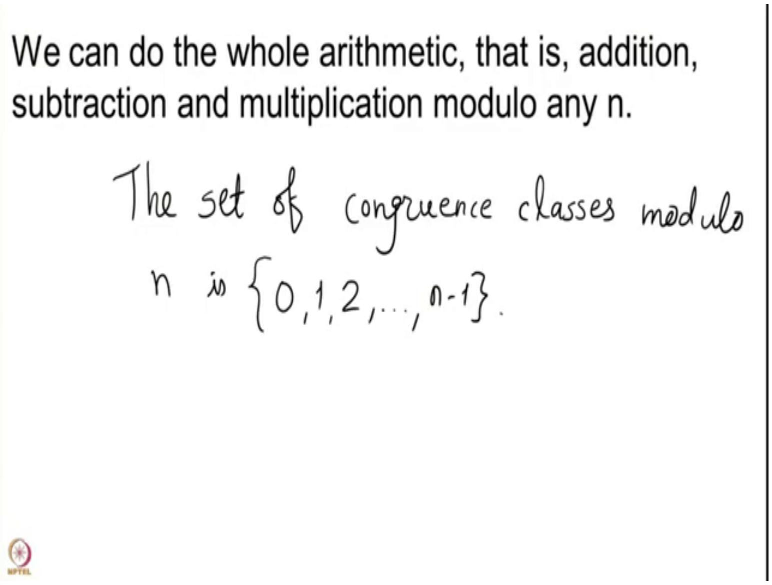
1 is congruent to 13, modulo 12, I think you should not really have any problem with this, the difference is minus 12, 1 minus 13 which is divisible by 12 or if you take the difference in the other way 13 minus 1 you get the difference to be 12 and which is the multiple of 12. Let us go to the next number minus 3, minus 3 is congruent to 9, modulo 12 because if I take the difference, if I subtract minus 3 from 9, I get 9 minus minus 3 which is 9 plus 3, which is already 12, which is then a multiple of 12. So, minus 3 is equal to 9, modulo 12.

So, this will tell you that you can use addition and subtraction while talking about congruence classes. We also have that 5 square is congruent to 1, modulo 12, 5 square is 25 and 25 is 1 plus 24, 24 is a multiple of 12, so 5 square is equal to 1 modulo 12, so using this we have been able to do some sort of arithmetic, we are able to.

This says that we can think about adding, subtracting and multiplying while remaining in the congruence modulo 12. So, what we have done is that we look at congruence modulo 12 and there we have only 12 numbers, any number is congruent modulo 12 to a number from 1, 2, 3, 4, 5, 6 up to 12, any number you take.

If you take 5 square which is 25 that is congruent to 1 modulo 12, if you take 13 this is congruent to 1 modulo 12. So, here we are able to find numbers which are less than or equal to 12 or you may replace 12 by 0. So, the set of congruence modulo 12 has only 12 elements 0, 1, 2, 3 up to 11 or you may think of it as 1, 2, 3 up to 12 and this set has the usual arithmetic properties.

(Refer Slide Time: 25:05)



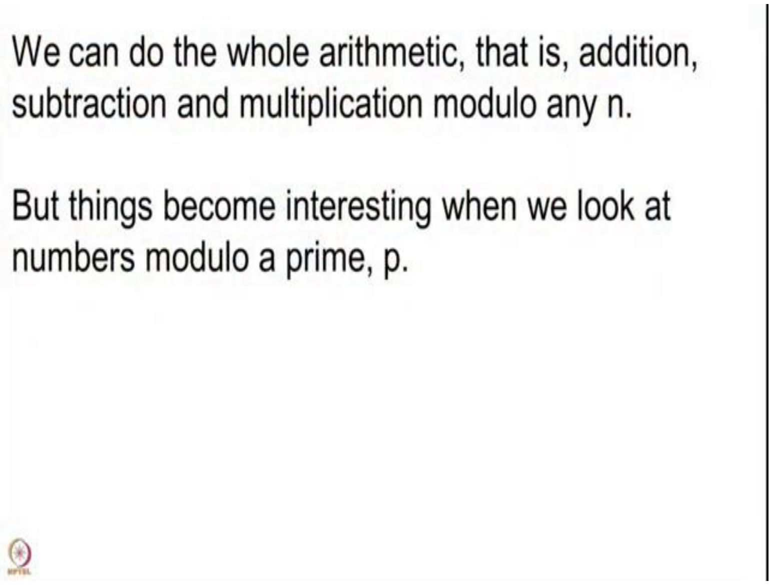
We can do the whole arithmetic, that is, addition, subtraction and multiplication modulo any n.

The set of congruence classes modulo n is $\{0,1,2,\dots,n-1\}$.

So, there is nothing (())(25:04) about 12, you can do the whole arithmetic which is addition, multiplication, subtraction modulo n, so that means the set you are going to look at will be the set, so the set of what are called congruence classes modulo n is 0, 1, 2, 1, 2 up to n minus 1, every natural number is congruent to one of these numbers and to a unique one such number.

And then within these numbers you can add, you can multiply, you can subtract and get one more number only in this form. So, this set, a very small set retains all these three properties of the natural numbers, you can ask can you divide and that may not be always possible. So, for instance can you divide 3 by 2 modulo 12, is there something which will give you 3 after having multiplied by 2 modulo 12 that answer is no, you cannot divide by 2 modulo 12.

(Refer Slide Time: 26:50)



We can do the whole arithmetic, that is, addition, subtraction and multiplication modulo any n.

But things become interesting when we look at numbers modulo a prime, p.

However, if you are looking at modulo classes, if you are looking at congruence classes, modulo of prime then things become very interesting, things will become very interesting when you look at numbers modulo a prime p, already the numbers modulo 2 which are 0 and 1 that itself already forms a very interesting set.

But what does one mean by this set being very interesting or what does one mean that you can do more, you can divide by non zero numbers and so on is something that we will see in the next lecture. See you until then, thank you.