

A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 33

Quadratic reciprocity law - I

Welcome back, we are studying the Legendre symbol which we have defined in particular to study quadratic residues modulo n . So, the Legendre symbol definition was somewhat complicated, it was defined with respect to a given odd prime p . And whenever we are given any natural number n or any integer n then we compute this Legendre symbol to be 0 1 or minus 1 we define it to be 0 1 or minus 1 depending on whether p divides a and in the remaining cases, we will take p to be not dividing a and then the Legendre symbol is 1 when a is a square modulo p and minus 1 when a is not a square modulo p . So, this is the way we have defined our Legendre symbol.

(Refer Slide Time: 01:19)

Theorem: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$

$$\alpha \in U_p, \quad \alpha^2 \in U_p$$

$$a, a^2, a^4, a^8, a^{16}, \dots$$

$$p=23$$

$$p-1/2=11$$



But in the last lecture, in the very last slide, we proved a result, which is a very remarkable result, which we have here on our slide, which tells us that the Legendre symbol a by p can be computed simply by computing a particular power of a modulo p . So, all we have to do is to compute this power of a modulo p and then we are done.

So, for instance, if you were to compute some Legendre symbol, often number a modulo some prime which is moderately high, then you would have to only compute this particular power,

which is also not a very difficult thing for a computer to compute, you know, what a computer typically can do very easily is that it can compute squares of elements quite easily.

So, whenever we are given any alpha in, say some U_p , then a computer would be able to compute alpha square for you. And, of course, this is something that we can use to compute all squares, but that would be too huge. If your prime is very big, then writing Q_p element wise will be very difficult.

So, instead what we are going to do is that, once we have this element a , we will compute a square, we will be able to compute square of a square which will give us a to the 4, we will be able to compute a to the 8, 8 to the 16th and so on as required. And after this, if we wanted to compute a certain power of a , you have to simply take product of certain elements from this sequence. For instance, if your p was 23 and then you have that p minus 1 by 2 is 11, then you have to take a raised to 8 into a square into a , the product of these three elements will give you a to the 11.

So, you have to compute a compute the square computed square and compute a power 8 and then take the product of these three that will give you a power 11 right away by doing these small computation. So, 1 2, 3 and then 4, 5 up in four computations, you would have computed a power 11. So, this is the way we are going to do the computations. Of course, here we will do the computations by hand, we will not be doing them using any computer, but we are going to follow the same method.

(Refer Slide Time: 03:55)

Examples:

1. Compute the Legendre symbol $\left(\frac{a}{p}\right)$ where $a = 5$ and $p = 23$.

$$\left(\frac{5}{23}\right) \equiv 5^{11} \pmod{23}.$$

$$5, 5^2 = 2, 5^4 = 4, 5^8 = 16$$

$$5^{11} = 5^8 \cdot 5^2 \cdot 5 = 16 \cdot 2 \cdot 5 = 9 \cdot 5 = 45$$

$$\left(\frac{5}{23}\right) = -1. \quad \equiv -1(23).$$



So, let us see some examples. We want to say let us say that we want to compute this Legendre symbol a by p where a is 5, and p is 23, the same thing that I had told you about earlier. So, this Legendre symbol we know is 5 power 11 modulo 23. So, to do this computation, we will compute these powers of 5, we have 5, we have 5 square which is 25 and therefore modulo 23 this is equal to 2 then we will compute 5 to the 4 which is square of 2. So, that quantity is four and further we compute 5 power 8 which is four square. So, this is 16. And therefore 5 power 11 for us is 5 power 8 into 5 square into 5. So, this is 16 into 2 into 5. So, 16 into 2 into 5, 16 into 2 is 32, which modulo 23 is 9.

So, we have nine into 5, which gives you 45 and now we see that this is congruent to minus 1 modulo 23. So, our answer is that the Legendre symbol of 5 with respect to 23 is minus 1. So, we do not have to check whether there are, we do not have to compute the 11 squares modulo 23. And then observe that 5 does not figure in any of those 11, in that set consisting of those 11 elements, and therefore, 5 must be a non square and hence its Legendre symbol is minus 1. This is the calculation which we avoid by using this formula that the Legendre symbol of a by p is simply a certain power of a modulo p .

(Refer Slide Time: 06:15)

Examples: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

2. Compute the Legendre symbol $\left(\frac{a}{p}\right)$ where $a = 6$ and $p = 31$.

$$\left(\frac{6}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right) \quad \frac{31-1}{2} = 15$$
$$2^{15} = 2 \cdot 2^2 \cdot 2^4 \cdot 2^8 = 2 \cdot 4 \cdot 16 \cdot 256$$
$$\equiv 4 \cdot 32 \cdot 8 \equiv 1 \pmod{31}.$$

Let us do 1 more computation where a is 6, and p is 31. Let us do this computation, where we are going to use both the results, 2 of have the results that we have proved earlier. And those results will be used in the following way. So, we first observe that the Legendre symbol of 6 with respect to 31 is the product of these 2 legendary symbols. Because we can write 6 as 2 into 3, so we will have that the legendary symbol of 6 is the product of the Legendre symbols of 2 and 3.

And now we will need to compute the 2 power 15 and 3 power 15. Remember 31 minus 1 by 2 is 15. So, we will also use so the 2 results that we are going to use here are the following that a by p is a by p into b by p . And we will also use this result that a by p is congruent to a to the power p minus 1 by 2 modulo p .

So, in Up, if we do the computations, then we are going to simply have to compute the 15th power of each a , so we will need to compute 2 power 15 and then we will also need to compute 3 power 15. So, let us begin with the competition of 2 power 15. As we have observed in the previous slide also the 15th power is simply the product of these four quantities.

Here 2 is simply 2, 2 square is four, 2 to the power 4 is the square of 4, so that is 16. And further 2 to the power 8 is the square of 16 so we get to 256. But among these, we will have to look at their modulo 31. So, when you look at it, modulo 31, 16 into 2 gives you 32, which is only 1. So, you are left with four into 256, 256 says 2 raise to 8, so that is 2 raise to 5 into 2 raise to three

and 2 raised to 5 is 32 and 2 raised to 3 is 8. So, this is again 32 square 32 into 32. And so this is simply congruent to 1 modulo 31.

So, 2 is actually a square modulo 31. You can also think of it in the following way that when you compute the square of 8, that is 64 and 64 is 2 modulo 31 because 62 is a multiple of 31. You remove that from 64 and you get the number to be 2 so 2 is a square modulo 31. So, the Legendre symbol for 2 by 31 is indeed 1.

(Refer Slide Time: 09:33)

Examples: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$

2. Compute the Legendre symbol $\left(\frac{a}{p}\right)$ where $a = 6$ and $p = 31$.

$$\left(\frac{6}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right) \quad \frac{31-1}{2} = 15$$

$$= 1 \cdot (-1) = -1$$

$$2^{15} = 2 \cdot 2^2 \cdot 2^4 \cdot 2^8 = 2 \cdot 4 \cdot 16 \cdot 256$$

$$\equiv 4 \cdot 32 \cdot 8 \equiv 1 \pmod{31}.$$

$$3^{15} = 3 \cdot 9 \cdot (-12) \cdot 20 = (-2) \cdot (-108) = (-2) \cdot (-15)$$

$$\equiv -1 \pmod{31}$$

Now, we need to compute the Legendre symbol for three. So, 3 power 15 will be 3 into 3 square which is 9 into 3 power four which is 9 square 9 square is 81. But 81 is between 62 and 93. These are the multiples of 31. And it is closer to 93. So, we will write this as minus 12, 81 plus twelve gives you 0 modulo 31. So, 81 is minus 12, and then we need to compute the square of the earlier number.

So, earlier number being minus 12, its square is 144. But 144 is 124 plus 20 and therefore modulo 31, these numbers are simply 20. Now, when you compute the product, top six, the 20 into 3, you get 60, and 60 is minus 2. When you compute the product of 9 and minus 12, you get minus 108.

But once again, you will take away 93, from 108, to get this as minus 2 into minus 15. And finally, you get 30, which is congruent to minus 1 mod 31. So, we therefore get that these numbers are 1 into minus 1, and therefore, the final answer is minus 1.

So, we can compute the Legendre symbol of 6 by 31, quite easily. Otherwise taking the 15th power of 6, that also would be a very difficult quantity, that would be a very difficult computation to do. And if you were to look at all the squares modulo 31, you would have to compute squares of all elements, or at least half of them, and you would have gotten 15 elements and then you would have realized that 6 does not figure in them. And therefore 6 is a quadratic non residue.

But this competition alone has reduced our number of competitions very much and to a manageable number. This is how we are going to do the competitions. But we would like to have further formally. Suppose I were to look at the quadratic residue of 2 modulo each prime, do I have to compute this power every time? Or is there a simpler formula telling me that if the prime is of this form, then 2 is a quadratic residue? And if the prime is of that form, then 2 is not a quadratic residue? Is there a formula like this, yes, there is a nice such formula. This is part of what are called the quadratic reciprocity laws.

(Refer Slide Time: 12:40)

Clearly, from the previous result,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$



So, we will go towards proving them. But note one of the simplest possible laws from here, which is that from the previous theorem, that we have proved when you take a to be any integer,

we have noted that the residue symbol the Legendre symbol, a by p is congruent to a power p minus 1 by 2 modulo p . And therefore, when you take a equal to minus 1, we get this particular result.

(Refer Slide Time: 13:31)

Clearly, from the previous result,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

± 1 ± 1

But we get the equality in above result, not a congruence.

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow (-1)^{p-1/2} = 1.$$



So, we get that minus 1 over p is congruent to minus 1 to the power p minus 1 by 2, this will also tell you that we get equality, we do not get a congruence and the reason for this is the following fact that this is either plus 1 or minus 1. And of course, all powers of minus 1 are also plus 1 and minus 1. So, when you have plus 1 here, you should have plus 1 here, because minus 1 sub p equal to 1 if and only if the other side gives you 1. Because if this were 1 and this were minus 1, then you would have that the difference of 1 and minus 1 being 2 is divisible by an odd prime, which is not possible.

So, here because the numbers are 1 and minus 1, the differences can be 0 or 2 or minus 2. Therefore, since p is an odd prime the difference is only allowed to be 0, so instead of congruence, we have an exact equality on the nodes, we can compute the Legendre symbol of minus 1 with respect to any prime simply by observing whether p minus 1 by 2 is even or not.

(Refer Slide Time: 14:49)

Clearly, from the previous result,

$$\begin{aligned}\left(\frac{-1}{p}\right) &\equiv (-1)^{(p-1)/2} \pmod{p}. \\ &= 1 \Leftrightarrow \frac{p-1}{2} \text{ is even} \Leftrightarrow p \equiv 1 \pmod{4}.\end{aligned}$$

But we get the equality in above result, not a congruence.

We further see a result for computing the Legendre symbol of 2 wrt an odd prime p .

So, here, we will, of course see a formula for 2 also but I will just let you that this is 1 if and only if p minus 1 by 2 is even. So, this is true if and only if we know that p is congruent to 1 modulo 4, among the primes which are odd p is either congruent to 1 modulo 4 or it is congruent to 3 modulo 4. So, whenever p is congruent to 1 modulo 4 minus 1 is a quadratic residue and whenever p is congruent to 3 modulo 4 minus 1 is a quadratic non residue.

(Refer Slide Time: 15:46)

Theorem: If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

equivalently, $2 \in Q_p$ if and only if $p \equiv \pm 1 \pmod{8}$.

Proof:

Now, what we do is to find the result for computing the Legendre symbol of 2 with respect to an odd prime p and this is that beautiful result.

(Refer Slide Time: 15:50)

Clearly, from the previous result,

$$\begin{aligned}\left(\frac{-1}{p}\right) &\equiv (-1)^{(p-1)/2} \pmod{p}. \\ &= 1 \iff \frac{p-1}{2} \text{ is even} \iff p \equiv 1 \pmod{4}.\end{aligned}$$

But we get the equality in above result, not a congruence.

We further see a result for computing the Legendre symbol of 2 wrt an odd prime p .

So, the earlier page that we have seen, this is called the first part of the quadratic reciprocity law.

(Refer Slide Time: 15:58)

Theorem: If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

equivalently, $2 \in Q_p$ if and only if $p \equiv \pm 1 \pmod{8}$.

Proof:

The result for 2 is called the second part of the quadratic reciprocity law. So, this will tell you that 2 is a square modulo p if and only if p is congruent to plus 1 or minus 1 modulo 8. So, all you have to observe is what is left for p once you go modulo 8, if what you are left with is 1 or minus 1. So for instance, if you were to take p equal to 31, then we know that 31 is congruent to minus 1 modulo 8, because once you divide by 8, 8 into 3 is 24, and 7 is left or 8 into 4 is 32.

And therefore, you have minus 1 and then by this result, 2 has to be a quadratic residue. So, this way, we can reduce our computations further.

(Refer Slide Time: 17:03)

Proof (contd.):

$$\begin{aligned}
 1 &\equiv (-1)^{\underbrace{(p-1)}_{\text{even}}} \pmod{p} \\
 2 &\equiv (-1)^2 \cdot \underbrace{2}_{\text{even}} \pmod{p} \\
 3 &\equiv (-1)^3 \cdot \underbrace{(p-3)}_{\text{even}} \pmod{p} \\
 &\vdots \\
 \frac{p-1}{2} &\equiv (-1)^{\frac{p-1}{2}} \cdot \underbrace{\frac{p+1}{2}}_{\text{even}} \pmod{p}
 \end{aligned}$$

all the numbers up to $\frac{p-1}{2}$

Once we prove this result, the proof of this result is also quite nice. So, I request you to pay close attention to this proof the proof is given in the following way. So, we observed that 1 is congruent to minus 1 into p minus 1 mod p and 2 is congruent to minus 1 square into 2 mod p, 3 is congruent to minus 1 cube into p minus 3 mod p and so on. So, if you observe this carefully, what we are doing on this side is that we are writing all the elements which are up to p minus 1 by 2.

So, our last number here would be p minus 1 by 2 congruent to minus 1 to the power p minus 1 by 2, and here we would have p plus or minus 1 by 2. So, I will explain what we are looking at mod p. The elements on the left hand side are all the numbers up to p minus 1 by 2. So, these are exactly half the numbers that we are writing on the left hand side and on the right hand side, observe that p is odd. So, this is even, 2 is an even quantity p minus 3 is even because p is odd, so on up to this.

So, we will choose the sign here, whether it is p plus 1 by 2 or p minus 1 by 2, depending on when we get the even quantity. So, if p plus 1 by 2 is even, then p minus 1 by 2 will have to be an odd number because it is 1 less than p plus 1 by 2 and therefore here you would get minus 1.

(Refer Slide Time: 19:29)

Proof (contd.):

$$\begin{aligned}
 1 &\equiv (-1)^{\underbrace{(p-1)}_{\text{even}}} \pmod{p} \\
 2 &\equiv (-1)^2 \cdot \underbrace{2}_{\text{even}} \pmod{p} \\
 3 &\equiv (-1)^3 \cdot \underbrace{(p-3)}_{\text{even}} \pmod{p} \\
 &\vdots \\
 \frac{p-1}{2} &\equiv (-1)^{\frac{p-1}{2}} \cdot \underbrace{\left(\frac{p+1}{2}\right)}_{\text{even}} \pmod{p}
 \end{aligned}$$

all the numbers up to $\frac{p-1}{2}$ (left side)

all even numbers up to $p-1$ (right side)

$$-\left(\frac{p+1}{2}\right) \equiv \frac{p-1}{2} \pmod{p}$$

$\frac{p+1}{2}$ is even \Leftrightarrow $\frac{p-1}{2}$ is odd

So, observe that $p + 1$ by 2 is even if and only if a very simple statement, $p - 1$ by 2 is odd. So, when I have $p + 1$ by 2 here, this is going to be minus 1 because it is minus 1 to the power an odd number. And I am indeed going to get minus of $p + 1$ by 2 to be $p - 1$ by 2 modulo p .

And if $p + 1$ by 2 is odd, or in other words, if $p - 1$ by 2 is even. So, if we choose the minus sign here, then of course, this will become plus 1, because it is minus 1 to the power an even quantity. So, here we have on this side, we get all the even numbers, which are also less than p . So, here we get all even numbers, up to $p - 1$, on the left hand side, we have all the numbers up to $p - 1$ by 2 . So, if I were to take product on the left hand side, I will get $p - 1$ by 2 factorial.

(Refer Slide Time: 21:15)

Proof (contd.): We take products on both sides to get

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{1+2+3+\dots+\frac{p-1}{2}} 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$



We take products on both sides to get $(p-1)!!$, this is going to be congruent to on the right hand side, you remember that there were minus 1 to the power 1 plus 2 plus 3 plus dot dot up to $p-1$ by 2. This was the sign on the right hand side, and then we had product of all even numbers up to $p-1$. And therefore, we had these to be $2^{p-1/2}$ into $(p-1)!!$.

(Refer Slide Time: 22:22)

Proof (contd.):

$$\begin{aligned} 1 &\equiv (-1)^{\underbrace{(p-1)}_{\text{even}}} \pmod{p} \\ 2 &\equiv (-1)^2 \cdot \underbrace{2}_{\text{even}} \pmod{p} \\ 3 &\equiv (-1)^3 \cdot \underbrace{(p-3)}_{\text{even}} \pmod{p} \\ &\vdots \\ \frac{p-1}{2} &\equiv (-1)^{\frac{p-1}{2}} \underbrace{\left(\frac{p+1}{2}\right)}_{\text{even}} \pmod{p} \end{aligned}$$

all the numbers up to $\frac{p-1}{2}$ } all even numbers up to $p-1$.

$$-\left(\frac{p+1}{2}\right) \equiv \frac{p-1}{2} \pmod{p}$$

$\frac{p+1}{2}$ is even $\Leftrightarrow \frac{p-1}{2}$ is odd

$1 \leq i \leq \frac{p-1}{2}$
 $= 2i$

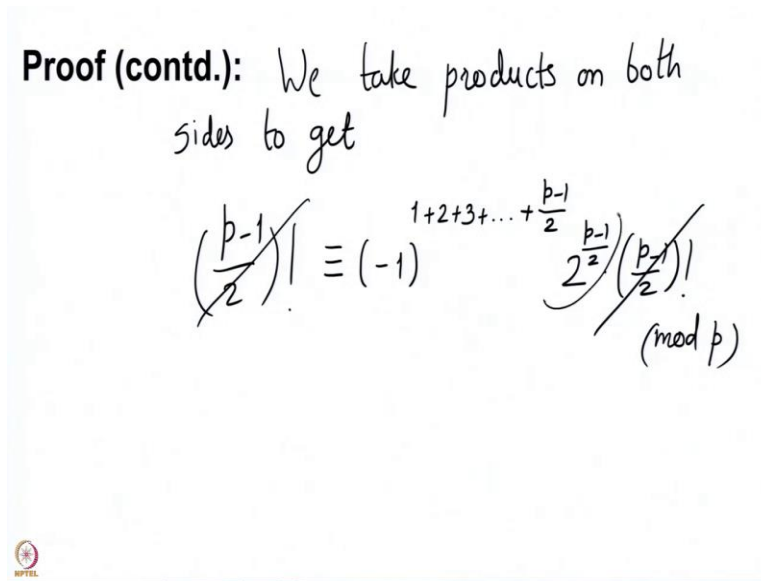


So, the product on the right hand side of all even numbers, these are given by, so, these are given by the 2 times the each of these being an even is given by $2i$ where you have i up to p

minus 1 by 2. And, of course, you will start from 1, the value for i will start from 1, and it will go up to p minus 1 by 2. So, there is a 2, which you can take common from each of the terms on the right when you take the product. So, the 2 will come p minus 1 by 2 times. And then what is left is simply 1 into 2 into 3 up to p minus 1 by 2. And that is the p minus 1 by 2 factorial.

(Refer Slide Time: 23:18)

Proof (contd.): We take products on both sides to get

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{1+2+3+\dots+\frac{p-1}{2}} 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$


So, we have the equality of these things modulo p . But then we observe that these 2 numbers can be cancelled out because these are both non 0 and 2 to the p minus 1 by 2 is either 1 or minus 1. So, we will just multiply it to that number by itself and we have it on the other side.

(Refer Slide Time: 23:40)

Proof (contd.): We take products on both sides to get

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{1+2+3+\dots+\frac{p-1}{2}}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$
$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{8}} \pmod{p}$$

Since p is odd $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}}$ \square

So, we have 2 to the p minus 1 by 2 being congruent to minus 1 and this is an arithmetic progression. And I leave it to you to figure out that its product is really p square minus 1 by 8. So, this sum is really p square minus 1 by 8 mod p . But since both sides are plus or minus 1, and p is odd, this is equal to the Legendre symbol 2 by p . But since p is odd for 2 by p and minus 1 to the power p square minus 1 by 8, we get an equality.

So, this allows us to compute the Legendre symbol for the integer 2 with respect to any odd prime. And now this is exact, this is going to be 1 exactly when p square minus 1 by 8 is an integer. It is an even integer. And therefore, this is true only when p is plus or minus 1 modulo 8. And this is the way we get our final formally and so, the only thing that now remains to compute is to compute the Legendre symbol of an odd prime with respect to an odd prime.

So, what we are going to do in that case is to try to reduce the competition's to smaller number using a certain reciprocity, if q is another order prime, then we will see how to relate the quadratic, the Legendre symbol q by p to the legendary symbol p by q . And that way we are going to reduce this competition further. So, we will do this in the next lecture. See you until then, thank you.