Today is the last class! Yay!

Two more weeks until the fall classes! Good luck with preparations.

I posted an activity titled Jacobi's symbol in this week's folder. It shows the steps for finding (3/p) and introduces a generalization of the Legendre symbol: Jacobi symbol.

This activity is not required. If you missed previous in-class/pre-class activity work and would like to make those up, feel free to work on it. You can print, write on it and scan. Or write on the PDF file.

Properties of Legendre symbol (fill in blanks and proofs)

ii) See pre-class.

iii) Same idea as $\left(\frac{4}{p}\right)=1$ in pre-class.

iv) see pre-class (Cian's work)

v) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \equiv (ab)^{p-1/2} \pmod p$ by Euler's criterion

$$\equiv a^{p-1/2}\ b^{p-1/2} \pmod p$$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

So $p \mid \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ But each # on RHS is ± 1, so their difference is ± 2 or 0. Since p is an odd prime, difference must be 0.

Properties of Legendre symbol continued (fill in blanks and proofs)

vi) For quadratic residues, $\left(\frac{a}{p}\right) = 1$.

For quadratic non-residues, $\left(\frac{a}{p}\right) = -1$.

For $a=0$, $\left(\frac{a}{p}\right) = 0$.

There are $\left(\frac{p-1}{2}\right)$ quadratic residues, $\left(\frac{p-1}{2}\right)$ non-residues.

So all of $\left(\frac{a}{p}\right)$ added gives

$$\underbrace{\left(\frac{p-1}{2}\right)}_{\text{from quadr. residues}} + \underbrace{\left(\frac{p-1}{2} \cdot (-1)\right)}_{\text{from quadr. non-residues}} + 0 = 0.$$

1

Using the properties of the Legendre symbol, simplify and evaluate the following.

(169 / 347) = 1 because 169 = 13^2.

(- 25 / 101) = -1 because (- 25 / 101) = (-1 / 101) * (25 / 101) = -1 * 1 = -1

(193 / 337) = -1 because (193 / 337) = (-144 / 337) = (12^2 / 337) * (-1 / 337) = 1 * +1 = -1

Hmm... Wolfram Alpha doesn't agree with the (-1/101) calculation: https://www.wolframalpha.com/input/?i=legendre+symbol+%28-1%2F101%29

(- 25 / 101) = 1 because (- 25 / 101) = (-1 / 101) * (25 / 101) = (100 / 101) * (25 / 101) = 1 * 1 = 1. Whoops! missed that

Yep! And we can also use that -1 is a square mod 1+4k t find (-1/101)=1.

- Miah :)

2
a,b,c

a)

2 is a square mod 7, so (2/7) should be 1.

The multiples of 2 up to (7-1)/2 are: 2, 4, and 6. They cannot be reduced mod 7.

7/2=3.5, and there are 2 multiples greater than 3.5, 4 and 6, so s=2.

Then, (2/7)=(-1)^2=1.

b)

(3/11) should be 1 because 3 is a square mod 11.

The multiples of 3 up to (11-1)/2 are: 3, 6, 9, 12, 15.

Reduced mod 7 the multiples are: 3,6, 9, 1, 4.

p/2=5.5, and there are 2 multiples greater than 5.5, 6 and 9, so s=2.

Then, (3/11)=(-1)^2=1.

c)

(2/11) should be -1 because 2 is not a square mod 11.

The multiples of 2 up to (11-1)/2 are: 2, 4, 6, 8, 10. They cannot be reduced mod 11.

11/2=5.5, and there are 3 multiples greater than 5.5; 6, 8, and 10; so s=3.

Then, (2/11)=(-1)^3=-1.

-Maggie

3 (all parts) This is long but they all use the same idea, so it didn't make sense to split. If you have any questions on this, feel free to email me.

For the other cases swap out at * and '

If p=8K+1 then there are 4k* multiples of 2 we need to use and we want to count the ones over 4K+.5'

out of 2, 4, 6, ... , 8K-2, 8K. 2K* of them are over half and so

(-1)^(2K) = 1

p=8K+3
4K+1*
4K+1.5'

2K+1* are over half

(-1)^(2K+1) = -1

p=8K+5
4K+2*
4K+2.5'

2K+1* are over half

(-1)^(2K+1) = -1

p=8K+7
4K+3*
4K+3.5'

2K+2* are over half

(-1)^(2K+2) = 1

Cian

4 a,b

4 a. $\left(\frac{11}{31}\right)\cdot\left(\frac{31}{11}\right) = (-1)^{10\cdot 30/4} = -1$ So $\left(\frac{11}{31}\right) = -1.$

$\left(\frac{31}{11}\right) = \left(\frac{9}{11}\right) = 1$ b/c $9 = 3^2$

4 b. $\left(\frac{41}{103}\right)\underbrace{\left(\frac{103}{41}\right)}_{=1} = (-1)^{40\cdot 102/4} = 1$

must be 1

$\left(\frac{103}{41}\right) = \left(\frac{21}{41}\right) = \left(\frac{3}{41}\right)\left(\frac{7}{41}\right) = (-1)(-1) = 1$

$\left(\frac{3}{41}\right)\underbrace{\left(\frac{\cancel{41}\,2}{3}\right)}_{-1} = (-1)^{40\cdot 2/4} = 1$

must be -1

$\underbrace{\left(\frac{7}{41}\right)}_{\text{must be } -1}\underbrace{\left(\frac{\cancel{41}\,6}{7}\right)}_{-1} = (-1)^{40\cdot 6/4} = 1$

-1 b/c -1 is a nonresidue for $p = 4k+3$

4 c

I refuse to use -2 instead of 101!!!

if that was what you meant by other way

$$\left(\frac{101}{103}\right) = -1 = (101)^{51} \bmod 103$$

$$\left(\frac{101}{103}\right)\left(\frac{103}{101}\right) = (-1)^{(101-1)(103-1)/4}$$

$$\left(\frac{101}{103}\right)\left(\frac{2}{101}\right) = 1$$

$$-1$$

$$\left(\frac{101}{103}\right)(-1) = 1$$

4 d

$$\left(\frac{42}{997}\right) = \left(\frac{7}{997}\right)\left(\frac{3}{997}\right)\left(\frac{2}{997}\right)$$

$$\begin{array}{cccc} \uparrow & \uparrow & \uparrow & \uparrow \\ 1 & -1 & 1 & -1 \leftarrow \text{Thm 2} \end{array}$$

$$\left(\frac{7}{997}\right)\left(\frac{997}{7}\right) = (-1)^{6\cdot 996/4}$$

$$\left(\frac{7}{997}\right)\left(\frac{3}{7}\right) = 1$$

$-1 \quad -1$

$$\left(\frac{3}{997}\right)\left(\frac{997}{3}\right) = (-1)^{2\cdot 996/4}$$

$$\left(\frac{3}{997}\right)\left(\frac{1}{3}\right) = 1$$

$1 \quad 1$

997 is not one away from a multiple of 8 so theorem 2 says that the last legendre symbol is -1.

I agree :)

Last page (No 4e)