MATH 136—**HOMEWORK** 4

Ricardo J. Acuña

(862079740)

1 Find all the quadratic residues of 3

x	x^2
0	$0 \equiv 0 (\mathrm{mod}\ 3)$
1	$1 \equiv 1 (\mathrm{mod}\ 3)$
2	$4 \equiv 1 (\mathrm{mod}\ 3)$

This table gives all the possible values for a square mod 3.

So the only quadratic residue of 3 is 1.

1 Find all the quadratic residues of 19

x	x^2
0	$0 \equiv 0 \pmod 3$
1	$1 \equiv 1 \pmod 3$
2	$4 \equiv 4 \pmod 3$
3	$9 \equiv 9 \pmod 3$
4	$16 \equiv 16 \pmod 3$
5	$25 \equiv 6 \pmod 3$
6	$36 \equiv 17 \pmod 3$
7	$49 \equiv 11 \pmod 3$
8	$64 \equiv 7 \pmod 3$
9	$81 \equiv 5 \pmod 3$
10	$100 \equiv 5 \pmod 3$
11	$121 \equiv 7 \pmod 3$
12	$144 \equiv 11 \pmod 3$
13	$169 \equiv 17 \pmod 3$
14	$196 \equiv 6 \pmod 3$
15	$225 \equiv 16 \pmod 3$
16	$256 \equiv 9 \pmod 3$
17	$289 \equiv 4 \pmod 3$
18	$324 \equiv 1 \pmod 3$

This table gives all the possible values for a square mod 19.

So the quadratic residues of 19 are 1,4,5,6,7,9,11,16, and 17.

Note: Jose said 0 is not considered a quadratic residue

3 Find all the values of Legendre symbol $\left(\frac{j}{7}\right)$ for $j = 1, 2, 3, 4, 5, 6$

x	x^2
0	0 $\equiv$ 0 (mod 3)
1	1 $\equiv$ 1 (mod 3)
2	4 $\equiv$ 4 (mod 3)
3	9 $\equiv$ 2 (mod 3)
4	16 $\equiv$ 2 (mod 3)
5	25 $\equiv$ 4 (mod 3)
6	36 $\equiv$ 1 (mod 3)

So, reading the table of squares modulo 7 we have:

$\left(\frac{1}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right) = 1$ since they're all quadratic residues. And, $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$ since they're not quadratic residues.

4 Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$ by using Euler's criterion.

$\left(\frac{7}{11}\right) = 7^{\frac{\phi(11)}{2}}(\text{mod}11) \overset{\text{11 is prime}}{=} 7^{\frac{11-1}{2}}(\text{mod}11) = 7^5(\text{mod}11) = 16807 \equiv 10 = 10 - 11 \equiv -1(\text{mod}11)$

5 Let a and b be integers not divisible by p. Show that either one or all of the three integers a,b and ab are quadratic residues of p.

Slu .

p does not divide $a \implies \left(\frac{a}{p}\right) \neq 0$

$\implies \left(\frac{a}{p}\right) = 1$ or $\left(\frac{a}{p}\right) = -1$

p does not divide $b \implies \left(\frac{b}{p}\right) \neq 0$

$\implies \left(\frac{b}{p}\right) = 1$ or $\left(\frac{b}{p}\right) = -1$

The evaluation of the possibilities for the Legendre symbol for a and b establishes are three possibilities for one of the pair a and b being a quadratic residue of p. Either a and b are quadratic residues of p. Either a or b is a quadratic residue of p. Or neither a nor b are quadratic residues of p. In that case we want to show ab is a quadratic residue of p.

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = 1$

So, either one or all of the three integers a,b and ab are quadratic residues of p.

■

6 Let p be a prime and a be a quadratic residue of p. Show that if $p \equiv 1(\text{mod} 4)$, then $-a$ is also a quadratic residue of p, whereas if $p \equiv 3(\text{mod} 4)$, then $-a$ is a quadratic nonresidue of p.

Slu .

$\left(\frac{-a}{p}\right) = \left(\frac{(-1)(a)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) \cdot 1 = \left(\frac{-1}{p}\right)$ Since a is a quadratic residue of p.

For the first case: $p \equiv 1 \pmod 4 \implies p-1 \equiv 0 \pmod 4 \implies \exists k \in \mathbb{Z} : p-1 = 4k \implies \frac{p-1}{2} = \frac{4k}{2} = 2k$

$\implies \frac{p-1}{2}$ is even

So, since p is prime by Euler's criterion $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\text{even}} = 1(\text{mod} p)$.

So, $-a$ is a quadratic residue modulo p.

For the first case: $p \equiv 3 \pmod 4 \implies p-1 \equiv 2 \pmod 4 \implies \exists k \in \mathbb{Z} : p-1 = 4k+2 \implies \frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$

$\implies \frac{p-1}{2}$ is odd

So, since p is prime by Euler's criterion $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\text{odd}} = -1(\text{mod} p)$.

So, $-a$ is a quadratic nonresidue modulo p.

■

7 Show that if p is an odd prime and a is an integer not divisible by p then $\left(\frac{a^2}{p}\right) = 1$.

Slu .

Since, either a is a quadratic residue modulo p, and a is not divisible by p. We can say $\left(\frac{a}{p}\right) = \pm 1$

$\left(\frac{a^2}{p}\right) = \left(\frac{(a)(a)}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = (\pm 1)^2 = 1(\text{mod } p)$

So, if p is an odd prime and a is an integer not divisible by p then $\left(\frac{a^2}{p}\right) = 1$.

■