CRYPTOGRAPHY HANDOUT 13

SQUARE ROOTS AND SQUARES

Based on Number Theory Through Inquiry (Marshall, Odell, and Starbird).

Question 1. *Determine which of the numbers* $1, 2, 3, \cdots, 12$ *are perfect squares modulo 13. For each such square, list the number or numbers in the set whose square is that number (i.e. its square roots).*

Number	*Square* mod13*?*	*Square Root(s)?*
1	*Yes*	$12^2 \bmod 13 \equiv 1 \bmod 13$
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

How many numbers (out of the 12) show up as squares mod13*?*

Definition. If a is an integer, p is a prime, and $a \equiv b^2 \mod p$ for some integer b, then a is called a **quadratic residue modulo** p. If a is not congruent to any square modulo p, then a is a **quadratic non-residue modulo** p.

Theorem 1. *Let p be a prime. Half the numbers not congruent to $0 \bmod p$ in a complete residue system $\mod p$ are quadratic residues and half are quadratic non-residues.*

Definition. For an odd prime p and a natural number a with p not dividing a, the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined to be:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue } \mod p \\ -1 & a \text{ is a quadratic non-residue } \mod p \end{cases}$$

Theorem 2. *Suppose p is an odd prime and p does not divide the numbers a or b. Then*

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

Rewrite the above theorem in your own words, so you remember what it means:

Euler's Criterion (Theorem). Suppose p is an odd prime and p does not divide the natural number a. Then a is a quadratic residue mod$p$ if and only if $a^{(p-1)/2} \equiv 1 \bmod p$, and a is a quadratic non-residue mod$p$ if and only if $a^{(p-1)/2} \equiv -1 \bmod p$.

Question 2. *Fill out the following table for* $p = 7$.

a	$a^{(p-1/2)} \equiv a^3 \bmod 73$?	$a^2 \bmod 7$
1	*1*	*1*
2		
3		
4		
5		
6		
12		

You should notice that you only have 1 *and* $-1 \bmod p$ *in the second column.*

Note. 1 is always a quadratic residue. You might wonder about other numbers too. Let's start by looking at -1:

Theorem 3. *Let* p *be an odd prime. Then* -1 *is a quadratic residue* mod$p$ *if and only if*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & p \equiv 3 \bmod 4 \end{cases}$$

Theorem 4. *Let* p *be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & p \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

Rather than looking at $\left(\frac{3}{p}\right), \left(\frac{4}{p}\right), \cdots$, we'll consider $\left(\frac{p}{q}\right)$ for primes p and q.

Question 3. *Fill out the following table assuming that the columns are p and the rows are q (ignore the boxes with x). You should only have 1 and -1.*

	3	5	7	11	13	17	19	23	29	31
3	x									
5		x								
7			x							
11				x						
13					x					
17						x				
19							x			
23								x		
29									x	
31										x

Question 4. *Using the table you made, make a conjecture about the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$.*