20- Squares Modulo p

Q1. Make a list of all the quadratic residues and all the nonresidues modulo 19.

Answer-

A number a is called a quadratic residue (QR) mod p if there exists an integer x such that :

$$x^2 \equiv a \pmod{p}$$

Otherwise, *a* is called a quadratic nonresidue (NR) mod p.

b	b^2
1	$1^2 \equiv 1$
2	$2^2 \equiv 4$
3	$3^2 \equiv 9$
4	$4^2 \equiv 16$
5	$5^2 = 25 \equiv 6$
6	$6^2 = 36 \equiv 17$
7	$7^2 = 49 \equiv 11$
8	$8^2 = 64 \equiv 7$
9 = (19-1)/2	$9^2 = 81 \equiv 5$

mod (19)

List of all the QRs modulo 19:

1,4,5,6,7,9,11,16,17

List of all the NRs modulo 19:

2,3,8,10,12,13,14,15,18

Q2. For each odd prime p, we consider the two numbers

$$A = \text{sum of all } 1 \le a < p \text{ such that } a \text{ is a quadratic residue modulo } p,$$

$$B = \text{sum of all } 1 \le a < p \text{ such that } a \text{ is a nonresidue modulo } p.$$

(a) Make a list of A and B for all odd primes p < 20.

(b) What is the value of A+ B? Prove that your guess is correct.

(c) Compute A mod p and B mod p. Find a pattern and prove that it is correct.

(d) Compile some more data and give a criterion on p which ensures that A= B.

Answer-

Odd primes p < 20 : 3,5,7,11,13,17,19

p	A	B	A + B	A (mod p)	B (mod p)
3	1	2	3	1	2
5	5	5	10	0	0
7	7	14	21	0	0
11	22	33	55	0	0
13	39	39	78	0	0
17	68	68	136	0	0
19	76	95	171	0	0

(a)

For p = 3, QR : {1} , NR : {2}

A = 1 , B = 2;

For p = 5, QRs : {1,4}, NRs : {2,3}

A = 1 + 4 = 5, B = 2 + 3 = 5;

For p = 7, QRs : {1,4,2}, NRs : {3,5,6}

A = 1 + 4 + 2 = 7, B = 3 + 5 + 6 = 14;

For p = 11, QRs : {1,4,9, 5, 3}, NRs : {2,6,7,8,10}

A = 1+4+9+5+3 = 22, B = 2+6+7+8+10= 33;

For p = 13, QRs : {1,4,9,3,12,10}, NRs : {2,5,6,7,8,11}

A = 1+4+9+3+12+10 = 39, B = 2+5+6+7+8+11= 39;

For p = 17, QRs : {1,4,9,16,8,2,15,13}, NRs : {3,5,6,7,10,11,12,14}

A = 1+4+9+16+8+2+15+13 = 68, B = 3+5+6+7+10+11+12+14= 68;

For p = 19, QRs : {1,4,9,16,6,17,11,7,5}, NRs : {2,3,8,10,12,13,14,15,18}

A = 1+4+9+16+6+17+11+7+5 = 76, B = 2+3+8+10+12+13+14+15+18= 95;

(b) A + B = $\frac{p(p-1)}{2}$

Proof - **A + B** = QRs mod p + NRs mod p

= 1 + 2 + ... + (p-1)

= $\frac{p(p-1)}{2}$

(c) If p =3 , A (mod p) = 1 and B (mod p) =2.

If p > 3 , then A ≡ 0(mod p) and B ≡ 0(mod p).

We know that there are exactly (p-1)/2 QRs mod p and they are

$1^2 , 2^2 , \ldots , \left(\frac{p-1}{2}\right)^2 \pmod p$

$A \equiv 1^2 , 2^2 , \ldots , \left(\frac{p-1}{2}\right)^2 \pmod p$

$$\equiv \frac{\left(\frac{(p-1)}{2}\right)\left(\frac{(p-1)}{2}+1\right)\left(2\frac{(p-1)}{2}+1\right)}{6} \pmod p$$

$$\equiv \frac{p\left(p^2-1\right)}{24} \pmod p \qquad \equiv pk \pmod p \quad \text{where } k = (p^2-1)/24 \text{ is an integer.} \quad (*)$$

$\equiv 0$ (since p divides $p(p^2 - 1)/24$)

(*) there are two reasons for k to be an integer.

(i) As p is an odd prime and 24 can't divide it. Therefore $(p^2 - 1)$ must be divisible by 24 .

(OR)

(ii) p is odd prime.

p is congruent to 1 (mod 4) or 3 (mod 4)

i.e. p = 4k +1 or 4k +3 , where k belongs to integer.

if we change mod to 3, then p is congruent to 1 (mod 3) or 2 (mod 3)

i.e p = 3m + 1 or 3m + 2, where m belongs to integer.

p	p-1	p+ 1	$p^2 - 1$
4k+1	4k	2(2k+1)	8k(2k+1)
4k+3	2(2k+1)	4(k+1)	8(2k+1)(k+1)
3m + 1	3m	(3m+2)	3m(3m+2)
3m + 2	3m+1	3(m+1)	3(3m+1)(m+1)

From the above table -

$p^2 - 1$ is divisible by 8 and 3 both. Therefore

$p^2 - 1$ is divisible by 8*3 =24.//

B = (A + B) – A

$$\equiv \frac{p(p-1)}{2} - \frac{p(p^2-1)}{24} \pmod{p}$$

$$\equiv p\left(\frac{p-1}{2} - \frac{p^2-1}{24}\right) \pmod{p}$$

$$\equiv 0$$

(d) A = B for p = 5, 13, 17.

Conjecture: If p ≡ 1 (mod 4) , then A =B.