Quiz 3

October 14, 2022

1. Prove that 3 is a quadratic residue of 23, but a nonresidue of 31.

Euler's criterion - Let p be an odd prime and $\gcd(a,p) = 1$. Then

$$a^{(p-1)/2} \equiv \begin{cases} 1 \pmod{p}, & a \text{ is QR,} \\ -1 \pmod{p}, & a \text{ is NR.} \end{cases}$$

$$\Rightarrow \quad 3^{(23-1)/2} \equiv 3^{11} \equiv (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv -5 \cdot 9 \equiv 1 \pmod{23}$$

$\Rightarrow$ 3 is quadratic residue of 23.

$$3^{(31-1)/2} \equiv 3^{15} \equiv (3^3)^5 \equiv (-4)^5 \equiv (-4)^3 \cdot 16$$

$$\equiv -2 \times 16 \equiv -32 \equiv -1 \pmod{31}$$

$\Rightarrow$ 3 is non residue of 31.

2. Compute the Legendre symbol

$$\left(\frac{143}{409}\right).$$

409 is a prime.

and 143 = 11 · 13

$\Rightarrow \left(\frac{143}{409}\right) = \left(\frac{11 \times 13}{409}\right) = \left(\frac{11}{409}\right)\left(\frac{13}{409}\right)$ $\left[\because \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\right]$

Quadratic Reciprocity Law. p & q - distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$$

$\Rightarrow \left(\frac{11}{409}\right) = \left(\frac{409}{11}\right)(-1)^{10/2 \cdot 408/2}$

$= \left(\frac{409}{11}\right) = \left(\frac{2}{11}\right)$ $\left[\because a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)\right]$

$= (-1)^{11^2-1/8}$ $\left[\because \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}\right]$

$= -1$

and $\left(\frac{13}{409}\right) = \left(\frac{409}{13}\right)(-1)^{12/2 \cdot 408/2}$

$= \left(\frac{409}{13}\right) = \left(\frac{6}{13}\right)$ $\left[\because a \equiv b \mod p \Rightarrow \left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \pmod{p}\right]$

$= \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)$ $\left[\because \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right]$

$= (-1)^{13^2-1/2} \left(\frac{13}{3}\right)(-1)^{12/2 \cdot 2/2}$ $[\because$ QR law$]$

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

$= -1$

$\Rightarrow \left(\frac{143}{409}\right) = \left(\frac{11}{409}\right)\left(\frac{13}{409}\right) = 1.$