Problem 1

Try to calculate $\left(\frac{10}{19}\right)$ using the $T(a,p)$ function. Notice you get the wrong answer. Why?

$$\begin{aligned}
T(10,19) &= \sum_{j=1}^{\frac{19-1}{2}} \left\lfloor \frac{10j}{19} \right\rfloor \\
&= \sum_{j=1}^{9} \left\lfloor \frac{10j}{19} \right\rfloor \\
&= \left\lfloor \frac{10}{19} \right\rfloor + \left\lfloor \frac{20}{19} \right\rfloor + \left\lfloor \frac{30}{19} \right\rfloor + \left\lfloor \frac{40}{19} \right\rfloor + \left\lfloor \frac{50}{19} \right\rfloor + \left\lfloor \frac{60}{19} \right\rfloor + \left\lfloor \frac{70}{19} \right\rfloor + \left\lfloor \frac{80}{19} \right\rfloor + \left\lfloor \frac{90}{19} \right\rfloor \\
&= 0+1+1+2+2+3+3+4+4 \\
&= 20
\end{aligned}$$

So, according to this, $\left(\frac{10}{19}\right)$ should be equal to $(-1)^{T(10,19)} = (-1)^{20} = 1$. However, this is, in fact, incorrect as $\left(\frac{10}{19}\right) = -1$. This is because 10 is even and not odd. The $T(a,p)$ function is only valid for odd a.

Problem 2

Evaluate $\left(\frac{945}{1009}\right)$ using:

(a) Legendre Symbols

(b) Jacobi Symbols

(a)

$$\begin{aligned}
\left(\frac{945}{1009}\right) &= \left(\frac{1009}{945}\right) \\
&= \left(\frac{64}{945}\right) \\
&= \left(\frac{2^6}{945}\right) \\
&= \left(\frac{2}{945}\right)^6 \\
&= (1)^8 \\
&= 1
\end{aligned}$$

(b)

$$\begin{aligned}
\left(\frac{945}{1009}\right) &= \left(\frac{1009}{945}\right) \\
&= \left(\frac{64}{945}\right) \\
&= \left(\frac{2^6}{3^3 \cdot 5 \cdot 7}\right) \\
&= \left(\left(\frac{2}{3}\right)^3 \cdot \left(\frac{2}{5}\right) \cdot \left(\frac{2}{7}\right)\right)^6 \\
&= \left(1^3 \cdot 1 \cdot 1\right)^6 \\
&= 1^6 \\
&= 1
\end{aligned}$$

Problem 3

Find the set of all primes for which 5 is a quadratic residue. The answer should be a set of congruences.

We are looking for primes p such that $\left(\frac{5}{p}\right) = 1$. Since $5 \not\equiv 3 \pmod 4$, this equals $\left(\frac{p}{5}\right)$. Since p is prime, $\forall p$, $p \not\equiv 0 \pmod 5$. Thus, we have 4 cases: $p \equiv 1, 2, 3,$ or $4 \pmod 5$. Let's find the quadratic residues of 5:

$$\begin{aligned}
1^2 &\equiv 1 \pmod 5 \\
2^2 &\equiv 4 \pmod 5 \\
3^2 &\equiv 4 \pmod 5 \\
4^2 &\equiv 1 \pmod 5
\end{aligned}$$

So, the quadratic residues of 5 are 1 and 4. Thus, 5 is a quadratic residue of p if and only if $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$.

Problem 4

Find the set of all primes for which 3 is a quadratic residue.

We are looking for primes p such that $\left(\frac{3}{p}\right) = 1$.

$$\begin{aligned}
\left(\frac{3}{p}\right) &= \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}\frac{3-1}{2}} \\
&= \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}
\end{aligned}$$

We can split this into two parts, one for $\left(\frac{p}{3}\right)$ and one for $(-1)^{\frac{p-1}{2}}$. Since p is prime, $\forall p$, $p \not\equiv 0 \pmod 3$. Thus, we have 2 cases for part 1: $p \equiv 1$ or $2 \pmod 3$. Let's find the quadratic residues of 3:

$$\begin{aligned}
1^2 &\equiv 1 \pmod 3 \\
2^2 &\equiv 1 \pmod 3
\end{aligned}$$

So, the quadratic residues of 3 are 1. Thus, $\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \equiv -1 \pmod 3 \end{cases}$. Now, for part 2, we can see that this is equivalent to $\left(\frac{-1}{p}\right)$, which we have proved $= \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \equiv -1 \pmod 4 \end{cases}$.

We want $\left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}\frac{3-1}{2}}$ to equal 1. This occurs when both parts $= 1$ or $= -1$. Thus, 3 is a residue if $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 3$ and $p \equiv -1 \pmod 4$. We can then combine these into two congruences: $p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$. Thus, 3 is a quadratic residue of p if $p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$.

Problem 5

Find the set of all primes for which -3 is a quadratic residue.

We are looking for primes p such that $\left(\frac{-3}{p}\right) = 1$.

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) \\
&= (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}} \\
&= \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}+\frac{p-1}{2}} \\
&= \left(\frac{p}{3}\right) \cdot (-1)^{p-1}
\end{aligned}$$

Since p is prime, $p-1$ will always be even, and $(-1)^{p-1} = 1$. Thus, we are left with finding $\left(\frac{p}{3}\right) = 1$. As we found in problem **4**, the quadratic residues of 3 are 1. Thus, -3 is a quadratic residue of p when $p \equiv 1 \pmod 3$.