Problem 1

Showing all work, compute $\left(\frac{10}{19}\right)$ using:

(a) Euler's Criterion

(b) Gauss' Lemma

(a)

$$\begin{aligned}
10^{\frac{19-1}{2}} &\equiv 10^9 \pmod{19} \\
&\equiv (10^2)^4 \cdot 10 \pmod{19} \\
&\equiv 100^4 \cdot 10 \pmod{19} \\
&\equiv 5^4 \cdot 10 \pmod{19} \\
&\equiv 25^2 \cdot 10 \pmod{19} \\
&\equiv 6^2 \cdot 10 \pmod{19} \\
&\equiv 36 \cdot 10 \pmod{19} \\
&\equiv 17 \cdot 10 \pmod{19} \\
&\equiv 170 \pmod{19} \\
&\equiv 18 \pmod{19} \\
&\equiv -1 \pmod{19}
\end{aligned}$$

(b)

$$\frac{19-1}{2} = 9$$

$$10, 20, 30, 40, 50, 60, 70, 80, 90$$

$$10, 1, 11, 2, 12, 3, 13, 4, 14 \text{ (take (mod 11))}$$

5 of these are greater than $\frac{19}{2}$, so $\left(\frac{10}{19}\right) = (-1)^5 = -1$.

Problem 2

Let p be an odd prime, and $(a, p) = 1$. Show that

$$\left(\frac{a}{p}\right) + \left(\frac{2a}{p}\right) + \left(\frac{3a}{p}\right) + \cdots + \left(\frac{(p-1)a}{p}\right) = 0$$

First, let there be a quadratic residue a such that $x^2 \equiv a \pmod{p}$ where x is a least nonnegative residue. Notice that if we input $-x$, $(-x)^2 \equiv x^2 \equiv a \pmod{p}$. So $-x$ gives the same quadratic residue a as x. So, for any quadratic residue a, there are two least residues x and $-x$ such that $x^2 \equiv a \pmod{p}$. Thus, since there are $p-1$ residues, the number of quadratic residues is $\frac{p-1}{2}$. Now, since legendre symbols are (sort of) multiplicative, we can the given equation as

$$= \left(\frac{a}{p}\right)\left(\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-2}{p}\right) + \left(\frac{p-1}{p}\right)\right)$$

As we found above, half of these are quadratic residues, and, consequently half are not quadratic residues. None of them $= 0$. Thus, half are $= 1$ and half are $= -1$. So the total sum of the inner legendre symbols are 0. Thus, we have:

$$\begin{aligned}
&= \left(\frac{a}{p}\right) \cdot 0 \\
&= 0
\end{aligned}$$

Problem 3

Determine the values c for which $3x^2 + 5x + c \equiv 0 \pmod{17}$ can be solved.

This quadratic has a solution if the discriminant is a quadratic residue. The discriminant is given by $5^2 - 4 \cdot 3 \cdot c = 25 - 12c$. We need to find c such that $25 - 12c \equiv r \pmod{17}$. Let's first find the quadratic residues modulo 17:

$$\begin{aligned}
0^2 &\equiv 0 \pmod{17}\\
1^2 &\equiv 1 \pmod{17}\\
2^2 &\equiv 4 \pmod{17}\\
3^2 &\equiv 9 \pmod{17}\\
4^2 &\equiv 16 \pmod{17}\\
5^2 &\equiv 25 \equiv 8 \pmod{17}\\
6^2 &\equiv 36 \equiv 2 \pmod{17}\\
7^2 &\equiv 49 \equiv 15 \pmod{17}\\
8^2 &\equiv 64 \equiv 13 \pmod{17}
\end{aligned}$$

$a^2 \equiv (a-17)^2 \pmod{17}$, so the other possible squares will not give any more unique quadratic residues. Thus, we have quadratic residues $0, 1, 2, 4, 8, 9, 13, 15, 16$. We can now find c such that $25 - 12c \equiv r \pmod{17}$.

$$\begin{aligned}
25 - 12c &\equiv r \pmod{17}\\
-12c &\equiv r - 25 \pmod{17}\\
5c &\equiv r + 9 \pmod{17}
\end{aligned}$$

The inverse of 5 modulo 17 is 7, so we can multiply both sides by 7 to get:

$$\begin{aligned}
5c &\equiv r + 9 \pmod{17}\\
c &\equiv 7(r + 9) \pmod{17}\\
c &\equiv 7r + 63 \pmod{17}\\
c &\equiv 7r + 12 \pmod{17}
\end{aligned}$$

Now we can plug in the quadratic residues to find c:

$$\begin{aligned}
r = 0 &\implies c \equiv 12 \pmod{17}\\
r = 1 &\implies c \equiv 19 \equiv 2 \pmod{17}\\
r = 2 &\implies c \equiv 26 \equiv 9 \pmod{17}\\
r = 4 &\implies c \equiv 40 \equiv 6 \pmod{17}\\
r = 8 &\implies c \equiv 68 \equiv 0 \pmod{17}\\
r = 9 &\implies c \equiv 75 \equiv 7 \pmod{17}\\
r = 13 &\implies c \equiv 103 \equiv 1 \pmod{17}\\
r = 15 &\implies c \equiv 117 \equiv 15 \pmod{17}\\
r = 16 &\implies c \equiv 124 \equiv 5 \pmod{17}
\end{aligned}$$

Thus, we have $c = \{0, 1, 2, 5, 6, 7, 9, 12, 15\}$.

Problem 4

Compute $\left(\frac{999}{2027}\right)$.

$$
\begin{aligned}
\left(\frac{999}{2027}\right) &= \left(\frac{3}{2027}\right)^3 \cdot \left(\frac{37}{2027}\right) \qquad (999 = 3^3 \cdot 37) \\
&= (\left(\frac{2027}{3}\right) \cdot (-1)^{\frac{3-1}{2}\frac{2027-1}{2}})^3 \cdot \left(\frac{2027}{37}\right) \qquad (2027 \not\equiv 3 \pmod 4) \\
&= (\left(\frac{2}{3}\right) \cdot -1)^3 \cdot \left(\frac{2027}{37}\right) \\
&= (-1 \cdot -1)^3 \cdot \left(\frac{29}{37}\right) \qquad (2^{\frac{3-1}{2}} \equiv 2 \equiv -1 \pmod 3) \\
&= 1 \cdot \left(\frac{37}{29}\right) \qquad (37 \not\equiv 3 \pmod 4) \\
&= 1 \cdot \left(\frac{8}{29}\right) \\
&= 1 \cdot \left(\frac{2}{29}\right)^3 \\
&= 1 \cdot ((-1)^{\frac{29^2-1}{8}})^3 \qquad \text{(By theorem proven in class)} \\
&= 1 \cdot ((-1)^{\frac{840}{8}})^3 \\
&= 1 \cdot ((-1)^{105})^3 \\
&= 1 \cdot (-1)^3 \\
&= 1 \cdot -1 \\
&= -1
\end{aligned}
$$