1. a) Suppose $n = p_1 \cdots p_k$ where the $p_j$ are distinct primes. Give a bound on the maximum number of possible solutions $x \pmod{n}$ to the equation:

$$a^m x^m + a_{m-1} x^{m-1} \cdots a_1 x + a_0 \equiv 0 \pmod{n}$$

where each $a_j \in \mathbb{Z}$ and $(a_m, n) = 1$. Explain your reasoning.

b) Count the number of solutions $x \pmod{40}$ to the equation

$$(x - 1)(x + 1) \equiv 0 \pmod{40}.$$ 

without explicitly finding them all, and explain your reasoning.

a) We see that

$$a^m x^m + a_{m-1} x^{m-1} \cdots a_1 x + a_0 \equiv 0 \pmod{n}$$

iff

$$a^m x^m + a_{m-1} x^{m-1} \cdots a_1 x + a_0 \equiv 0 \pmod{p_j} \forall p|n.$$ 

so we have a solution (mod $n$) if and only if we have a simultaneous solution (mod $p_j$) for each $1 \leq j \leq k$. Furthermore, if $c_j \pmod{p_j}$ is a solution (mod $p_j$) for $1 \leq j \leq k$ then by the Chinese Remainder Theorem we can find $x \equiv c_j \pmod{p_j}$ for each $j$ that is unique (mod $n$). We see that by Lagrange’s theorem there are at most $m$ distinct possible $c_j$s (mod $p_j$) for each $j$ and each set of $\{c_1, c_2, \ldots, c_k\}$ produces a distinct solution (mod $n$). So we see there are, at most, $m^k$ solutions (mod $n$).

b) As in part (a), we see that $(x - 1)(x + 1) \equiv 0 \pmod{40}$ iff $(x - 1)(x + 1) \equiv 0 \pmod{8}$ and (mod 5). We see $x \equiv \pm 1 \pmod{5}$ are solutions and, by Lagrange’s Theorem, we have that these must be the only solutions (mod 5). Since 8 is not prime, we have to check for more. In fact, we see that 8|(x - 1)(x + 1) iff $x$ is odd so we have the solutions $x \equiv 1, 3, 5, 7 \pmod{8}$. By the Chinese Remainder Theorem this means we can construct eight distinct solutions (mod 40).

2. Show 2 is a primitive root (mod 19).

We see that $2^2 \equiv 4 \pmod{19}$ and $2^3 \equiv 8 \pmod{19}$, $2^6 \equiv 7 \pmod{19}$ and $2^9 \equiv -1 \pmod{19}$. Since $(2, 19) = 1$, the order of 2 must divide $\phi(19) = 18$, but is not 1,2,3,6, or 9, so the order of 2 must be 18. Thus it is a primitive root.

3. Use primitive roots and indices to count the number of integer pairs $(x, y)$ (mod 19) that are solutions to

$$11x^6 \equiv y^7 \pmod{19}.$$
From the previous problem we know that 2 is a primitive root (mod 19). We also know that $2^3 \cdot 2^9 \equiv (8)(-1) \equiv 11$ (mod 19) so the index of 11 with respect to the primitive root of 2 is $3 + 9 = 12$. We have the trivial solution $x \equiv y \equiv 0$ (mod 19) and for every other solution we see $(x, 19) = (y, 19) = 1$. So we can take the indices of $x$ and $y$:

$$11x^6 \equiv y^7 \quad (\text{mod } 19) \Rightarrow 12 + 6\text{ind}(x) \equiv 7\text{ind}(y) \quad (\text{mod } 18).$$

Since $(12, 18) = 6$ and $(7, 6) = 1$, we only have solutions when $6|\text{ind}(y)$, and (mod 18) there are only 3 such values for $\text{ind}(y)$: 6, 12, and 18. In those cases the equation reduces to

$$2 + \text{ind}x \equiv 7\frac{\text{ind}(y)}{6} \quad (\text{mod } 3) \Rightarrow \text{ind}(x) \equiv 1 + \frac{\text{ind}y}{6} \quad (\text{mod } 3)$$

which has a unique solution in $\text{ind}(x)$ (mod 3) and thus 6 different solutions for $\text{ind}(x)$ (mod 18). So three possible values for $y$ with six possible values of $x$ for each, along with the trivial (0,0) solution gives 19 possible solutions.

4. a) Suppose a primitive root, $g$, exists (mod $m$). Show that for $n \in \mathbb{N}$, $g^n$ is a primitive root (mod $m$) if and only if $(n, \phi(m)) = 1$.

b) Prove that for any $m \in \mathbb{N}_{\geq 2}$, the number of primitive roots (mod $m$) is either 0 or $\phi(\phi(m))$.

a) Suppose $(n, \phi(m)) = d > 1$ then $(g^n)^{\frac{\phi(m)}{d}} = (g^{\frac{m}{d}})^{\phi(m)} \equiv 1$ (mod $m$) by Euler’s Theorem. Thus $g^n$ has order that divides $\phi(m)/d < \phi(m)$ so $g^n$ is not primitive.

If $(n, \phi(m)) = 1$ then $(g^n)^k = g^{nk} \equiv 1$ (mod $m$) for any $k \in \mathbb{N}$ then since $g$ is a primitive root we have $\phi(m)|nk$ but $(n, \phi(m)) = 1$ so $\phi(m)|k$. Thus the smallest $k$ can be is $\phi(m)$, which works by Euler’s Theorem, so $g^n$ is indeed a primitive root.

b) From part (a) we see that if a primitive root, $g$, exists (mod $m$) then all the primitive roots are $g^n$ where $1 \leq n \leq \phi(m)$ and $(n, \phi(m)) = 1$, and there are $\phi(\phi(m))$ such $n$. So the number of primitive roots is either 0 or $\phi(\phi(m))$.

5. For any odd prime, $p$, let $g$ be a primitive root (mod $p$), which we have shown to always exist.

a) Use indices to show that $g^n$, for $n \in \mathbb{N}$, is a quadratic residue (mod $p$) if and only if $n$ is even.

b) Use part (a) to provide an alternate proof of Euler’s Criterion.

a) We see that, taking indices with respect to $g$ (mod $p$) we have

$$g^n \equiv x^2 \quad (\text{mod } p) \iff n \equiv 2\text{ind}(x) \quad (\text{mod } p - 1)$$
which, since \(2|(p - 1)\), this has a solution if and only if \(2|n\). Thus \(g^n\) is a quadratic residue if and only if \(n\) is even.

b) Let \(r = \frac{1}{2}(p - 1)\). We see \(g^r \equiv -1\) since \((g^r)^2 = g^{2r} \equiv 1 \pmod{p}\) and \(g^r \not\equiv 1 \pmod{p}\). If \(n\) is even then \(nr\) is a multiple of \(p - 1\) and so \((g^n)^r = g^{nr} \equiv 1 \pmod{p}\). If \(n\) is odd then \(nr \equiv r \pmod{p - 1}\) so \((g^n)^r = g^{nr} \equiv g^r \equiv -1\).

Thus we see that
\[
(g^n)^r \equiv \left(\frac{g^n}{p}\right) \pmod{p}
\]
and for every \(a\) with \((a, p) = 1\) we have \(a = g^n\) for some \(n \in \mathbb{N}\) so
\[
a^r \equiv \left(\frac{a}{p}\right) \pmod{p}
\]
and thus we’ve proven Euler’s Criterion.

6. a) Show that if \(n = n_1 n_2\) for odd \(n_1, n_2 \in \mathbb{Z}\) then
\[
\frac{1}{2}(n - 1) \equiv \frac{1}{2}(n_1 - 1) + \frac{1}{2}(n_2 - 1) \pmod{2}
\]
and
\[
\frac{1}{8}(n^2 - 1) \equiv \frac{1}{8}(n_1^2 - 1) + \frac{1}{8}(n_2^2 - 1) \pmod{2}
\]

b) Use part (a) and the properties of the Legendre symbol to show that for odd \(n \in \mathbb{N}\) that the Jacobi symbol satisfies:
\[
\left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(n-1)} \quad \text{and} \quad \left(\frac{2}{n}\right) = (-1)^{\frac{1}{4}(n^2-1)}.
\]

c) Use part (a) and the Law of Quadratic Reciprocity to show that for odd \(n, m \in \mathbb{N}\) with \((m, n) = 1\) that the Jacobi symbol satisfies:
\[
\left(\frac{n}{m}\right) \left(\frac{m}{n}\right) = (-1)^{\frac{1}{2}(n-1)(m-1)}
\]

[Hint: Start by showing this for \(m = p\) prime and proceed from there.]

a) We note that
\[
\frac{1}{2}(n - 1) \equiv \frac{1}{2}(n_1 - 1) + \frac{1}{2}(n_2 - 1) \pmod{2} \iff n_1n_2 - 1 \equiv n_1 + n_2 - 2 \pmod{4}
\]
and so we just check that the later equality holds for \((n_1, n_2) = (1, 1), (1, 3), (3, 1), \) and \((3, 3)\), which are all the odd pairs \((mod\ 4)\).
Similarly we note that
\[
\frac{1}{8}(n^2 - 1) \equiv \frac{1}{2}(n_1^2 - 1) + \frac{1}{2}(n_2^2 - 1) \pmod{2} \iff n_1^2n_2^2 - 1 \equiv n_1^2 + n_2^2 - 2 \pmod{16}
\]
The only odd squares (mod 16) are 1 and 9 so we just check the later equality holds for \((n_1^2, n_2^2) = (1, 1), (1, 9), (9, 1),\) and \((9, 9),\) which are all the odd square pairs (mod 16). Thus we've shown both equalities hold.

**b)** We will prove these statements by induction on the number of prime factors of \(n\).

We know both equalities hold when \(n = p\) is prime by properties of the Legendre symbol, so suppose these equalities hold for all \(n\) with at most \(k\) prime factors. Then if \(n = p_1 \cdots p_k p_{k+1}\) not necessarily distinct primes and \(m = p_1 \cdots p_k\), we have
\[
\left(\frac{-1}{n}\right) = \left(\frac{-1}{m}\right) \left(\frac{-1}{p_{k+1}}\right) = (-1)^{\frac{1}{2}(m-1)+\frac{1}{2}(p_{k+1}-1)} = (-1)^{\frac{1}{2}(mp_{k+1}-1)} = (-1)^{\frac{1}{2}(n-1)}
\]
and
\[
\left(\frac{2}{n}\right) = \left(\frac{2}{m}\right) \left(\frac{2}{p_{k+1}}\right) = (-1)^{\frac{1}{2}(m^2-1)+\frac{1}{2}(p_{k+1}^2-1)} = (-1)^{\frac{1}{2}(m^2 p_{k+1}^2-1)} = (-1)^{\frac{1}{2}(n^2-1)}
\]
using the equivalences in part (a) and so we have the claim by induction.

**c)** First we will verify this by induction on the number of prime factors of \(n\) when \(m = p\) is prime. This is quadratic reciprocity when \(n = q\) is prime, so suppose
\[
\left(\frac{n}{p}\right) \left(\frac{p}{n}\right) = (-1)^{\frac{1}{2}(n-1)(p-1)}
\]
holds when \(n\) has at most \(k\) prime factors. Then if \(n = q_1 \cdots q_k q_{k+1}\) not necessarily distinct primes and \(r = q_1 \cdots q_k\), we have
\[
\left(\frac{n}{p}\right) \left(\frac{p}{n}\right) = \left(\frac{r}{p}\right) \left(\frac{p}{r}\right) \left(\frac{q_{k+1}}{p}\right) \left(\frac{p}{q_{k+1}}\right) = (-1)^{\frac{1}{2}(r-1)(p-1)+\frac{1}{2}(q_{k+1}-1)(p-1)}
\]
\[
= (-1)^{\frac{1}{2}(p-1)\left(\frac{1}{2}(r-1)+\frac{1}{2}(q_{k+1}-1)\right)} = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q_{k+1}-1)} = (-1)^{\frac{1}{2}(p-1)(n-1)}
\]
again using the equalities from (a) which proves the claim when \(m = p\) is prime. Now suppose we have it when \(m\) has at most \(k\) prime factors, then if \(m = p_1 \cdots p_{k+1}\) with \(s = p_1 \cdots p_k\), we have
\[
\left(\frac{n}{m}\right) \left(\frac{m}{n}\right) = \left(\frac{n}{s}\right) \left(\frac{s}{n}\right) \left(\frac{p_{k+1}}{n}\right) \left(\frac{n}{p_{k+1}}\right)
\]
\[
= (-1)^{\frac{1}{2}(n-1)\left(\frac{1}{2}(s-1)+\frac{1}{2}(p_{k+1}-1)\right)} = (-1)^{\frac{1}{2}(n-1)\frac{1}{2}(sp_{k+1}-1)} = (-1)^{\frac{1}{2}(n-1)(m-1)}
\]
which proves the claim for all \(m\), and so we’re done.
7. Check to see if 42, 101, and 1234 are quadratic residues (mod 31337). [Note: 31337
is a prime.] Show your work when computing Legendre or Jacobi symbols, though you
don’t have to show long-division steps when computing remainders (just be careful, or
use a calculator for that).

First we observe that $31337 \equiv 1 \pmod{8}$ which means that \( \left( \frac{2}{31337} \right) = \left( \frac{-1}{31337} \right) = 1 \) and
we can invert via quadratic reciprocity without picking up a minus sign so

\[
\left( \frac{42}{31337} \right) = \left( \frac{2}{31337} \right) \left( \frac{3}{31337} \right) \left( \frac{7}{31337} \right) = \left( \frac{31337}{3} \right) \left( \frac{31337}{7} \right) \\
= \left( \frac{2}{3} \right) \left( \frac{5}{7} \right) = -\left( \frac{7}{5} \right) = -\left( \frac{2}{5} \right) = -(-1) = 1
\]

so 42 is a quadratic residue (mod 31337). Also

\[
\left( \frac{101}{31337} \right) = \frac{31337}{101} = \left( \frac{27}{101} \right) = \left( \frac{3}{101} \right)^3 = \left( \frac{3}{101} \right) = \left( \frac{101}{3} \right) = \left( \frac{2}{3} \right) = -1
\]

so 101 is not a quadratic residue (mod 31337). Finally

\[
\left( \frac{1234}{31337} \right) = \left( \frac{2}{31337} \right) \left( \frac{617}{31337} \right) = \left( \frac{31337}{617} \right) = \left( \frac{487}{617} \right) = \left( \frac{617}{487} \right) = \left( \frac{130}{487} \right) \\
= \left( \frac{2}{487} \right) \left( \frac{5}{487} \right) \left( \frac{13}{487} \right) = \left( \frac{487}{5} \right) \left( \frac{487}{13} \right) = \left( \frac{2}{5} \right) \left( \frac{6}{13} \right) =
- \left( \frac{2}{13} \right) \left( \frac{3}{13} \right) = \left( \frac{1}{3} \right) = 1
\]

and so 1234 is a quadratic residue (mod 31337).

8. Compute the Jacobi Symbol

\[
\left( \frac{15}{11345467650427} \right).
\]

where 11345467650427 is not a prime. Show your work. Does this tell us whether or
not 15 is a quadratic residue (mod 11345467650427)? We have

\[
\left( \frac{15}{11345467650427} \right) = \left( \frac{3}{11345467650427} \right) \left( \frac{5}{11345467650427} \right) \\
= - \left( \frac{11345467650427}{3} \right) \left( \frac{11345467650427}{5} \right) = - \left( \frac{1}{3} \right) \left( \frac{2}{5} \right) = 1
\]
This alone is not enough information to verify if 15 is a quadratic residue (mod 11345467650427), since the Jacobi symbol can only confirm that a number is not a quadratic residue.

9. Let $p$ be an odd prime. Show that the equation

$$x^2 + bx + c \equiv 0 \pmod{p}$$

for $b, c \in \mathbb{Z}$ has solutions in $x \in \mathbb{Z}$ if and only if

$$\left(\frac{b^2 - 4c}{p}\right) = 1 \quad \text{or} \quad b^2 - 4c \equiv 0 \pmod{p}$$

If $\left(\frac{b^2 - 4c}{p}\right) = 1$ or $b^2 - 4c \equiv 0$, then $b^2 - 4c$ is a quadratic residue (mod $p$) so let $y \in \mathbb{Z}$ be such that $y^2 \equiv b^2 - 4c$ (mod $p$). Since $p$ is odd, 2 is invertible (mod $p$) so choose $z \in \mathbb{Z}$ such that

$$z \equiv 2^{-1}(-b + y) \pmod{p}.$$

which is inspired by the quadratic equation. We see that

$$z^2 + bz + c \equiv 4^{-1}(b^2 - 2by + y^2) + 2^{-1}b(-b + y) + c$$

$$\equiv 4^{-1}(2b^2 - 2by - 4c) - 2^{-1}b^2 + 2^{-1}by + c \equiv 2^{-1}(b^2 - b^2 + by + by) - c + c \equiv 0 \pmod{p}$$

so indeed the polynomial has solutions (mod $p$).

Now suppose the polynomial has solutions (mod $p$), let $y \in \mathbb{Z}$ be a solution then

$$y^2 + by + c \equiv 0 \pmod{p} \Rightarrow 4(y^2 + by + c) \equiv 0 \pmod{p} \Rightarrow (2y + b)^2 - (b^2 - 4c) \equiv 0 \pmod{p}$$

so

$$(2y + b)^2 \equiv b^2 - 4c \pmod{p}$$

and so $b^2 - 4c$ is a quadratic residue (mod $p$), so $\left(\frac{b^2 - 4c}{p}\right) = 1$ or $p | (b^2 - 4c)$.

10. For any $N \in \mathbb{N}$, show for every prime $p | (4N^2 + 1)$ that $p \equiv 1 \pmod{4}$. Use this to show that there are infinitely many primes $p \equiv 1 \pmod{4}$.

If $p | (4N^2 + 1)$ then $4N^2 \equiv -1 \pmod{p}$ so $(2N)^2 \equiv -1 \pmod{p}$. Since $p$ must be odd we have $\left(\frac{-1}{p}\right) = 1$ which we know holds iff $p \equiv 1 \pmod{4}$, thus every prime dividing $4N^2 + 1$ is equivalent to 1 (mod 4).

Now let $p_1, \ldots, p_k$ be a finite list of distinct primes equivalent to 1 (mod 4) and let

$$N = p_1 \cdots p_k.$$ 

Then there exists some prime $q | (4N^2 + 1)$ that is not on that list but by the above claim is also equivalent to 1 (mod 4). We can add $q$ to the list and by induction we can make the list arbitrarily large, and so there are infinitely many such primes.