You must show all your work and explain your answers carefully. There is no credit for just writing down the answer, whether it is correct or not.

(1) **Divisibility by 7:** Let \( m = d_n d_{n-1} \ldots d_3 d_2 d_1 d_0 \) be an \( n \)-digit integer. (So for example 1287 has \( d_0 = 7, d_1 = 8, d_2 = 2, d_4 = 1 \). Recall that in class we showed that \( m \) is divisible by 11 if and only if \( \sum_{i=0}^{n} (-1)^i d_i \) is divisible by 11.

(a) Find a similar (though slightly more complicated) formula involving the digits of \( m \) which determines whether \( m \) is divisible by 7. (Hint: We worked out \( 10^i \mod 7 \) in class.)

**Solution:**

\[
\sum_{i=0}^{n} d_i 10^i \equiv \sum_{i=0}^{n} d_i 3^i \mod 7
\]

\[
\equiv d_0 + 3d_1 + 2d_2 + 6d_3 + 4d_4 + 5d_5 + d_6 + 3d_7 + \cdots \mod 7
\]

\[
\equiv d_0 + 3d_1 + 2d_2 - d_3 - 3d_4 - 2d_5 + d_6 + 3d_7 + \cdots \mod 7
\]

So \( m \) is divisible by 7 if and only if \( d_0 + 3d_1 + 2d_2 - d_3 - 3d_4 - 2d_5 + d_6 + 3d_7 + \cdots \) is divisible by 7. Note that the coefficients start to repeat with \( d_6 \).

(b) Use the ideas from the first part to determine the remainder when 1462783394 is divided by 7. No credit for calculator answers.

**Solution:**

\[
1462783394 \equiv 4 + 3 \cdot 9 + 2 \cdot 3 - 3 - 3 \cdot 8 - 2 \cdot 7 + 2 + 3 \cdot 6 + 2 \cdot 4 - 1 \mod 7
\]

\[
\equiv 23 \mod 7
\]

\[
\equiv 2 \mod 7
\]

and so the remainder is 2.

(2) Prove that the set of bitstrings of infinite length is uncountable.

**Solution:** The idea is to assume the set is countable, and find a contradiction (very similar to the proof that \( (0, 1) \) is uncountable). If the set is countable then the elements can be listed:

\[
d_1 = d_{11} d_{12} d_{13} d_{14} \ldots
\]

\[
d_2 = d_{21} d_{22} d_{23} d_{24} \ldots
\]

\[
d_3 = d_{31} d_{32} d_{33} d_{34} \ldots
\]

\[
d_4 = d_{41} d_{42} d_{43} d_{44} \ldots
\]

\[
\cdots \text{ etc.}
\]

where every \( d_{ij} \) is either 0 or 1. Then the bitstring \( d = a_1 a_2 a_3 a_4 \ldots \) is not on the list, where \( a_i = \overline{d}_{ii} \) because \( d \) differs from \( d_i \) in the \( i \)-position. Therefore the set is not countable, so it must be uncountable.
(3) Solve for $x$. Your answer should have the form $x \equiv a \mod m$ where $0 \leq a < m$.

(a) $30x \equiv 1 \mod 49$.

**Solution:** $\gcd(30, 49) = 1$ and $1 = 30 \cdot 18 + 49 \cdot (-11)$. So $x \equiv 18 \mod 49$.

(b) $2x \equiv 73 \mod 99$.

**Solution:** $\gcd(2, 99) = 1$ and $1 = 99 \cdot 1 + 2 \cdot (-49)$. Then $2 \equiv 50 \mod 99$, and so $x \equiv 2 \cdot 73 \equiv 50 \cdot 73 \equiv 86 \mod 99$.

(c) $9x \equiv 3 \mod 64$.

**Solution:** $\gcd(9, 64) = 1$ and $1 = 64 \cdot 1 + 9 \cdot (-7)$. Then $9 \equiv 57 \mod 64$ and so $x \equiv 9 \cdot 3 \equiv 43 \mod 64$.

(4) Prove the following results using mathematical induction. Note that we have already seen some of these results in previous worksheets/class but proved them using different methods, you must use induction to receive any credit.

(a) $P(n) : \sum_{i=1}^{n} (2i - 1) = n^2$

**Solution:**

Basis Step: $P(1)$ is true because $2 - 1 = 1^2$.

Inductive Step: Assume $P(n)$ is true for integer the $n$, then

$$\sum_{i=1}^{n+1} (2i - 1) = \sum_{i=1}^{n} (2i - 1) + (2n + 1)$$

$$= n^2 + (2n + 1) \text{ because } P(n) \text{ is true}$$

$$= (n + 1)^2$$

Therefore $P(n) \Rightarrow P(n+1)$ and so $P(n)$ is true for all $n \geq 1$ by induction.

(b) $P(n) : \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

**Solution:**

Basis Step: $P(1)$ is true because $1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6}$.

Inductive Step: Assume $P(n)$ is true for integer the $n$, then

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n + 1)^2$$

$$= \frac{n(n+1)(2n+1)}{6} + (n + 1)^2 \text{ because } P(n) \text{ is true}$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}$$

Therefore $P(n) \Rightarrow P(n+1)$ and so $P(n)$ is true for all $n \geq 1$ by induction.
(c) \( \sum_{i=1}^{n} i \cdot i! = (n+1)! - 1. \)

**Solution:**

Basis Step: \( P(1) \) is true because \( 1 \cdot 1! = 2! - 1. \)

Inductive Step: Assume \( P(n) \) is true for integer the \( n \), then

\[
\sum_{i=1}^{n+1} i \cdot i! = \sum_{i=1}^{n} i \cdot i! + (n+1) \cdot (n+1)!
\]
\[
= (n+1)! - 1 + (n+1) \cdot (n+1)! \text{ because } P(n) \text{ is true}
\]
\[
= (n+2) \cdot (n+1)! - 1
\]
\[
= (n+2)! - 1
\]

Therefore \( P(n) \Rightarrow P(n+1) \) and so \( P(n) \) is true for all \( n \geq 1 \) by induction.

(5) Show that if \( p \) is a prime number then the only solutions of \( x^2 \equiv 1 \mod p \) are \( x \equiv 1 \mod p \) and \( x \equiv (p-1) \mod p \). (You must first show that they are solutions, and then prove that there are no other solutions). Then, find an example where \( n \) is not prime such that \( x^2 \equiv 1 \mod n \) has other solutions besides \( x \equiv 1 \mod n \) and \( x \equiv n-1 \mod n \).

**Solution:** First verify that \( 1^2 \equiv 1 \mod p \) and \( (p-1)^2 \equiv p(p-2)+1 \equiv 1 \mod p \). To show these are the only solutions: If \( x^2 \equiv 1 \mod p \), then \( p|\left(x^2 - 1\right) \) and so \( p|(x-1)(x+1) \). We saw in class that if a prime number divides a product then it must divide one of the factors. If \( p|(x-1) \) then \( x \equiv 1 \mod p \) and if \( p|(x+1) \) then \( x \equiv -1 \equiv p-1 \mod p \).

If \( n = 8 \) then \( 3^2 \equiv 1 \mod 8 \) but \( 3 \not\equiv 1 \mod 8 \) and \( 3 \not\equiv n-1 \mod 8 \).

(6) Prove by mathematical induction that if \( A \) is a set with \( |A| = n \) and \( n \geq 2 \), then \( A \) has \( \frac{n^2 - n}{2} \) subsets which contain 2 elements. (Hint: Let \( A = \{1, 2, 3, \ldots, n\} \) and see what the pattern is for small values of \( n \) first.)

**Solution:** \( P(n) \): If \( A \) has \( n \) elements then it has \( \frac{n^2 - n}{2} \) subsets which contain 2 elements.

Basis Step: \( P(2) \) is true because a set \( A \) with two elements has \( 1 = \frac{2^2 - 2}{2} \) subsets which contains 2 elements (that is the set \( A \) itself).

Inductive Step: Assume \( P(n) \) is true for integer the \( n \), so that a set with \( n \) elements has \( \frac{n^2 - n}{2} \) subsets which contain 2 elements. We must show that \( P(n+1) \):

\( A \) set with \( n+1 \) elements has \( \frac{(n+1)^2 - (n+1)}{2} \) subsets which contain 2 elements) is true.

First note that \( \frac{(n+1)^2 - (n+1)}{2} = \frac{n(n+1)}{2} \), and put \( A = \{1, 2, \ldots, n\} \) and \( B = \{1, 2, \ldots, n, n+1\} \). There are two ways for a subset \( C \) of \( B \) to contain 2 elements. Either \( C \subseteq A \) or \( C \) consists of one element from \( A \) and the element \( n+1 \).
In the first case there are $\frac{n^2 - n}{2}$ subsets containing 2 elements because $A$ has $n$ elements and $P(n)$ is assumed to be true. In the second case there are $n$ choices for the element from $A$, so there are $n$ subsets of this form.

The total number of subsets of $B$ containing 2 elements is $\frac{n^2 - n}{2} + n = \frac{n(n + 1)}{2}$. Therefore $P(n) \Rightarrow P(n + 1)$ and so $P(n)$ is true for all $n \geq 2$ by induction.