1. (10 pts) Prove the following theorem:

THEOREM: If \( a, b, c, d \) are positive integers, and if \( a|b \) and \( c|d \), then \( ac|bd \).

Notes: (i) The notation \( x|y \) means \( x \) divides \( y \).
(ii) Show all steps in your proof (and, as usual, show all work).

\[
\begin{align*}
\text{If } a|b \iff b &= am_1, m_1 \in \mathbb{Z} \\
\text{and } c|d \iff d &= cm_2, m_2 \in \mathbb{Z}
\end{align*}
\]

Then, \( bd = ac (m_1 m_2) \) and since \( m_1 m_2 \in \mathbb{Z} \)

\[ \Rightarrow ac|bd. \]
2. (10 pts) Is the following statement true or false? If it is True, then supply a detailed PROOF. If it False, then prove that it is False by supplying a COUNTEREXAMPLE.

**STATEMENT:** If $a$, $b$ and $c$ are positive integers, and if $a|bc$, then either $a|b$ or $a|c$.

**FALSE:** Consider $a=6$, $b=2$, $c=3$. Then, $bc=6$ so $a|bc$ but $a \not| b$ and $a \not| c$. 
3. (15 pts) Prove or disprove the following statement:

**STATEMENT:** If \( a, b, m \) are positive integers, such that

\[
a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m},
\]

then

\[
a \cdot c \equiv b \cdot d \pmod{m}.
\]

Note: If the statement is TRUE, then supply a complete PROOF. If the statement is FALSE, then show that it is false, by supplying a COUNTEREXAMPLE.

\[
\text{TRUE:} \quad a \equiv b \pmod{m} \iff a = b + ms, \quad s \in \mathbb{Z}
\]

\[
c \equiv d \pmod{m} \iff c = d + mt, \quad t \in \mathbb{Z}
\]

Then,

\[
ac = (b + ms)(d + mt)
\]

\[
= bd + m(sd + bt) + m^2st
\]

\[
= bd + m[st + bt + ms]
\]

Since \( st + bt + ms \in \mathbb{Z} \) \( \Rightarrow \) \( ac \equiv bd \pmod{m} \).
4. (10 pts) Let \( h \) be the hashing function \( h(k) = k \mod 101 \). (I.e., \( h(k) \) is the smallest non-negative integer that is congruent to \( k \) modulo 101. This will be one of the integers: 0, 1, \ldots, 100). Then compute

\[
h(104578690).
\]

[HINT: We have that 100 \( \equiv -1 \mod 101 \). Therefore, 100\( x \equiv -x \mod 101 \), for any integer \( x \). Here’s how to use this, in computing \( h \) (any positive integer): For example, 5762 = 57 \times 100 + 62. Taking “\( x \)” above to be “57”, 5762 \( \equiv -57 + 62 = 5 \mod 101 \) so \( h(5762) = 5 \).]

\[
104578690 = 1045786 \times 100 + 90
\]
\[
\equiv -1045786 + 90
\]
\[
= -10457 \times 100 - 86 + 90
\]
\[
= -10457 \times 100 + 4
\]
\[
\equiv 10457 + 4
\]
\[
= 104 \times 100 + 57 + 4
\]
\[
= 104 \times 100 + 61
\]
\[
\equiv -104 + 61
\]
\[
= -100 - 4 + 61
\]
\[
= -100 + 57
\]
\[
\equiv 1 + 57 = 58 \mod 101.
\]

So \( h(104578690) = 58 \).
5. (10 pts) Consider the linear congruential generator

\[ x_{n+1} = (4x_n + 1) \mod 7 \]

with seed \( x_0 = 3 \).

(I.e., in more mathematical language, consider the sequence \( x_n, n \geq 0 \), defined by the recursion

\[ x_{n+1} = (4x_n + 1) \mod 7, n \geq 1, \]

obeying the initial condition \( x_0 = 3 \). Then compute all of the \( x_n, n \geq 0 \) explicitly.

[HINT: Start computing \( x_0, x_1, x_2, x_3, \ldots \); and pretty soon you’ll find it clear what all of them are.]

\[ \begin{align*}
  x_0 &= 3 \\
  \Rightarrow x_1 &= (4(3)+1) \mod 7 = 6 \\
  \Rightarrow x_2 &= (4(6)+1) \mod 7 = 4 \\
  \Rightarrow x_3 &= (4(4)+1) \mod 7 = 3 \\
  \Rightarrow x_4 &= 6 \\
  x_5 &= 4 \\
  x_6 &= 3.
\end{align*} \]
6. (15 pts) Recall that if \( n \) is any positive integer, then \( \phi(n) \) is the number of positive integers \( \leq n \) that are prime to \( n \). For example, to compute \( \phi(8) \), the positive integers \( \leq 8 \) are 1, 2, 3, 4, 5, 6, 7 and 8. Of these, only 1, 3, 5 and 7 are prime to 8. Therefore, \( \phi(8) = 4 \). \( \phi(n) \) is the Euler phi-function.

(i) (5 pts) Compute \( \phi(15) \).

\[ 15 = 3 \times 5 \]

\[ \Rightarrow 1, 2, 4, 7, 8, 11, 13, 14 \text{ are relatively prime to } 15. \]

\[ \Rightarrow \phi(15) = 8 \]

(ii) (10 pts) If \( p \) is any prime, compute \( \phi(p) \).

[HINT: Try a few primes; the general formula for any prime will soon become clear.]

If \( p \) is prime, then for all \( k = 1, 2, \ldots, p-1 \)

\[ \gcd(k, p) = 1 \Rightarrow \phi(p) = p - 1. \]
7. (15 pts)

(i) (3 pts) Convert the hexadecimal expansion \( \text{FA1E}_{16} \) to its binary expansion.

\[
\text{Hex: } \text{FA1E}_{16} \quad \Rightarrow \quad \text{Binary: } 1111\ 1010\ 1100\ 0001\ 1110
\]

(ii) (3 pts) Convert the hex number in (i) above into an octal number.

\[
\text{FA1E}_{16} = (0111\ 1110\ 0101\ 0000\ 0110)_2 = (3\ 7\ 2\ 6\ 0\ 3\ 6)_8
\]

(iii) (3 pts) Convert the hex number in (i) to a decimal number.

\[
\text{FA1E}_{16} = 15 \cdot 16^4 + 10 \cdot 16^3 + 12 \cdot 16^2 + 1 \cdot 16 + 14
\]

(iv) (3 pts) Convert the hex number in (i) to a binary number.

This is part (i).

(v) (3 pts) Convert the decimal number \((1326)_{10}\) into a binary number.

\[
1326 = 2 \cdot 663 + 0
\]
\[
663 = 2 \cdot 331 + 1
\]
\[
331 = 2 \cdot 165 + 1
\]
\[
165 = 2 \cdot 82 + 1
\]

Answers:

(i) \( \text{FA1E}_{16} \)
(ii) \( 3726036_8 \)
(iii) \( 15 \cdot 16^4 + 10 \cdot 16^3 + 12 \cdot 16^2 + 1 \cdot 16 + 14 \)
(iv) \( \text{FA1E}_{16} \)
(v) \( 1326 = (10100101110)_2 \)
8. (10 pts) We've shown in class that (*) \( 1 + x + \cdots + x^n = \frac{x^{n+1} - 1}{x-1} \), if \( x \neq 0 \). Use this to show that

\[
3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = \frac{3}{4} (5^{n+1} - 1),
\]

for any integer \( n \geq 0 \).

[HINT: Using equation (\(*\)) above, you don't have to go through a proof by induction again.]

\[
3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = 3(1 + 5 + 5^2 + \cdots + 5^n)
\]

\[
= 3 \cdot \frac{5^{n+1} - 1}{5 - 1}
\]

\[
= \frac{3}{4} (5^{n+1} - 1)
\]
9. (20 pts) Use induction on the integer \( n \), for \( n \geq 0 \), to show that

\[
1^2 + 3^2 + 5^2 + \cdots + (2n + 1)^2 = \frac{(n + 1)(2n + 1)(2n + 3)}{3}
\]

**Basis Step:** \( n = 0 \Rightarrow 1^2 = \frac{(0+1)(2(0)+1)(2(0)+3)}{3} \)

**Inductive Step:** Assume \( 1^2 + 3^2 + \cdots + (2k+1)^2 = \frac{(k+1)(2k+1)(2k+3)}{3} \)
for arbitrary \( k \geq 0 \). We show that

\[
1^2 + 3^2 + \cdots + (2k+1)^2 + (2k+3)^2 = \frac{(k+1)(2k+1)(2k+3) + (2k+3)^2}{3}
\]

\[
= \frac{(k+1)(2k+1)(2k+3) + 3(2k+3)^2}{3}
\]

\[
= \frac{2k+3 \left[ (k+1)(2k+1) + 3(2k+3) \right]}{3}
\]

\[
= \frac{2k+3 \left( 2k^2 + 9k + 10 \right)}{3}
\]

\[
= \frac{(k+1)(2k+1)(2k+3) + (2k+3)}{3}
\]

The desired result.
10. (15 pts) Prove, by induction on \( n \), that

\[ 2^n > n^2 \]

for every integer \( n \geq 5 \).

**Basis Step:** \( n=5 \Rightarrow 2^5 = 32 > 25 = 5^2 \).

**Inductive Step:** Assume for arbitrary integer \( k \geq 5 \),
\[ 2^k > k^2 \; \text{we show} \; 2^{k+1} > (k+1)^2. \]

\[ 2^{k+1} = 2 \cdot 2^k > 2k^2 \]
\[ = k^2 + k^2 \leq k^2 + 2k + 1 \]
\[ = (k+1)^2 \; \text{Note: if } k \geq 5, \]
\[ k^2 \geq 5k \Rightarrow 2k + 5 \geq 2k + 1 \]
11. (15 pts) Recall that an $r$-permutation of a set $S$ is a sequence $(x_1, \ldots, x_r)$ of $r$ different elements of $S$. E.g., (4,1,2) is a 3-permutation of \{1, 2, 3, 4, 5\}; but (4,1,4) is not since the elements in the sequence are not different.

An $r$-combination of a set $S$ is a subset of $S$ having exactly $r$ elements.

(i)(2pts) List all 2-permutations of \{1, 2, 3\}.
\[
(1,2), (2,1), (1,3), (3,1), (2,3), (3,2).
\]

(ii)(2pts) List all 3-combinations of \{1, 2, 3, 4\}.
\[
\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}.
\]

(iii)(2 pts) Compute $P(6, 3)$. [Note: You don’t have to multiply it out.]
\[
P(6, 3) = \frac{6!}{(6-3)!} = 120.
\]

(iv)(2 pts) Compute $C(5, 1) = \frac{5!}{4!} = 5$.

(v)(3 pts) Compute $C(5, 4) = \frac{5!}{4!} = 5$.

(vi)(4 pts) What is the number of all permutations of \{1, 2, 3, 4\}? [Recall that a permutation of a set $S$ is an $n$-permutation of $S$, where $n = |S|$.
\[
4! = 24
\]
12. (20 pts) Solve the lhrc (linear homogeneous recurrence relation with constant coefficients)

\[ a_n = -4a_{n-1} - 4a_{n-2}, n \geq 2 \]

obeying the initial conditions

\[ a_0 = 1, \ a_1 = 2. \]

NOTE: Show all steps and all work.

\[ r^2 + 4r + 4 = 0 \Rightarrow (r + 2)^2 = 0 \Rightarrow r = -2 \text{ (repeated)} \]

\[ \Rightarrow a_n = \alpha_1 (2)^n + \alpha_2 n (2)^n \]

\[ a_0 = 1 \Rightarrow 1 = \alpha_1. \]

\[ \alpha_1 = 2 \Rightarrow 2 = -2\alpha_1 - 2\alpha_2 \Rightarrow \alpha_1 + \alpha_2 = -1 \]

\[ \Rightarrow \alpha_2 = -1 - \alpha_1 = -2 \]

\[ \Rightarrow a_n = (\ldots) - 2n(\ldots) \]
13. (20 pts) Solve the hrce

\[ a_n = 6a_{n-1} - 9a_{n-2}, n \geq 2, \]

obeying the initial conditions:

\[ a_0 = 2, a_1 = -1. \]

[Again, show all work.]

\[ r^2 - 6r + 9 = 0 \Rightarrow (r - 3)^2 = 0 \]
\[ r = 3 \text{ (repeated)} \]

\[ a_n = a_1 3^n + a_2 n 3^n \]
\[ a_0 = 2 \Rightarrow \boxed{2 = a_1} \]
\[ a_1 = -1 \Rightarrow -1 = 3a_1 + 3a_2 \Rightarrow 3a_2 = -1 - 3a_1 \]
\[ = -1 - 6 = -7 \]
\[ \Rightarrow a_2 = -\frac{7}{3} \]

\[ a_n = 2 \cdot 3^n - \frac{7}{3} n 3^n \]