1. (10 points)

(a) (6 points) Prove there exist infinitely many primes.


(b) (4 points) What is the octal expansion of the integer with hexadecimal expansion \((12C)_{16}\)? Show all your work.

Work:
The first step is to find the binary expansion of \((12C)\) \(_{16}\). Since \(1 = (0001)\) \(_2\), \(2 = (0010)\) \(_2\), and \(C = 12 = (1100)\) \(_2\) we get

\[
(12C) = (0001|0010|1100) = (000100101100)\.
\]

The second step is to obtain the octal expansion of

\[
(000100101100) = (000100101100) = (0454)\.
\]

Answer: \((12C)_{16} = (454)\).
2. (10 points)

(a) (2 points) Find $3^{203}$ mod 11. Show all your work.

Solution: Fermat’s little Theorem gives $3^{10} \equiv 1 \pmod{11}$ (11 is a prime). Therefore

$$3^{203} \equiv (3^{10})^{20} \cdot 3 \equiv 1^{20} \cdot 27 \equiv 27 \equiv 5 + 2 \cdot 11 \equiv 5 \pmod{11}.$$  
Answer: $3^{173} = 5 \pmod{11}$.

(b) (8 points) The following system of congruences

$$\begin{cases} x & \equiv 1 \pmod{10} \\ x & \equiv -1 \pmod{17} \end{cases}$$

has a unique solution modulo a positive integer $m$. Write down $m$ (bottom of next page) and also find the smallest positive integer $x$ that satisfies both congruences. Show all your work. To receive full credit you must use methods developed in the course. Guessing or ad hoc methods will receive little credit.

Work: The Chinese Remainder Theorem states that $m = 10 \cdot 17 = 170$.

The unique solution modulo 170 is, in Webwork notation, given by

$$x \equiv a_1 \hat{m}_1 \hat{y}_1 + a_2 \hat{m}_3 \hat{y}_2 \pmod{170},$$

where $a_i$ is the “right hand side of the $i$th congruence”, $m_i$ is the “modulus of the $i$th congruence”, $\hat{m}_i = m/m_1$, and $\hat{y}_i$ is the inverse of $\hat{m}_i$ modulo $m_i$.

We immediately have $a_1 = 1$ and $\hat{m}_1 = 17$; $a_2 = -1$ and $\hat{m}_2 = 10$.

To find the $\hat{y}_i$ we “reverse Euclid’s algorithm for 10 and 17”.

$$17 = 10 + 7$$
$$10 = 7 + 3$$
$$7 = 2 \cdot 3 + 1.$$ 

Therefore

$$1 = 7 - 2 \cdot 3$$
$$= 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 2 \cdot 10$$
$$= 3 \cdot (17 - 10) - 2 \cdot 10$$
$$= 3 \cdot 17 - 5 \cdot 10.$$ 

So $\hat{y}_1 = 3$ and $\hat{y}_2 = -5$. Finally $x \equiv 1 \cdot 17 \cdot 3 + (-1) \cdot 10 \cdot (-5) \equiv 101 \pmod{170}$.

Answer: $m = 170$ and $x = 101$. 

3. (10 points)

(a) (4 points) You are given the following affine encryption cipher on the “canonical” residues mod 7: 0, 1, …, 6

\[ f(p) = 4p - 1 \mod 7. \]

Decrypt the ciphertext message “122” showing all your work. To receive full credit you must use methods developed in the course. Guessing or ad hoc methods will receive little credit.

**Solution:** The first step is to find the inverse \( f^{-1} \) of \( f \) modulo 7. If

\[ q \equiv f(p) \equiv 4p - 1 \mod 7, \]

then

\[ p \equiv 4^{-1}(q + 1) \equiv 2(q + 1) \mod 7 \]

and so \( f^{-1}(p) = 2(p + 1) \mod 7 \).

The next step is to apply \( f^{-1} \) to 1 and 2: \( f^{-1}(1) = 2(1+1) = 4 \) and \( f^{-1}(2) = 2(2+1) = 6 \mod 7 \).

So the original message was 466.

**Answer:** 122 is code for 466.

(b) (6 points) Prove that for all non-negative integers \( n \geq 1 \)

\[ \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}. \]

**Solution:** Proof by induction.

*Base case:* When \( n = 1 \), the identity reduces to \( 1^3 = \frac{1^2 \cdot 2^2}{4} \).

*Inductive step:* Assume the statement is true for \( n = k \) and deduce it for \( n = k + 1 \).

\[
\sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3 \\
= \sum_{i=1}^{k} i^2 + (k+1)^3 \\
= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\
= \frac{(k+1)^2(2k^2 + 4(k+1))}{4} \\
= \frac{(k+1)^2(2k^2 + 4k + 4)}{4} \\
= \frac{(k+1)^2(k+2)^2}{4}.
\]

\( \square \)