MAT 312     SUMMER II, 2014     MIDTERM

Solutions

Question 1.

a. Find all $n \in \mathbb{N}$, with $n \geq 2$, for which the following congruences hold.

(i) $13 \equiv 7 \mod n$,  (ii) $-1 \equiv 6 \mod n$,  (iii) $0 \equiv -3 \mod n$.

b. Find all $n \in \mathbb{N}$ such that $\phi(n) = 12$.

c. Prove that if an odd prime number can be expressed as $p = x^2 + y^2$ with integers $x$ and $y$ then $p \equiv 1 \mod 4$.

Solution.

a. (i). $13 \equiv 7 \mod n \Rightarrow 13 = k \cdot n + 7$ for some $k \in \mathbb{Z}$. Equivalently, $6 = k \cdot n$, or $n|6$. The divisors of 6 are 1, 2, 3 and 6. So, $n$ can be 2, 3 or 6.

(ii). $-1 \equiv 6 \mod n \Rightarrow -1 = k \cdot n + 6$ for some $k \in \mathbb{Z}$. Equivalently, $-7 = k \cdot n$, or $n|7$. The divisors of 7 are 1 and 7. So, $n$ is equal to 7.

(iii) $0 \equiv -3 \mod n \Rightarrow 0 = k \cdot n - 3$ for some $k \in \mathbb{Z}$. Equivalently, $3 = k \cdot n$, or $n|3$. The divisors of 7 are 1 and 3. So, $n$ is equal to 3.

b. Let us assume that $n = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ where $p_1$, $p_2$, \ldots, $p_r$ are distinct primes and $\alpha_i \in \mathbb{N}$ for all $i = 1, \ldots, r$. Then

\[
\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \ldots \phi(p_r^{\alpha_r}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_r^{\alpha_r - 1}(p_r - 1).
\]

Note that $p_i^{\alpha_i - 1}(p_i - 1) \neq p_j^{\alpha_j - 1}(p_j - 1)$ since $p_i \neq p_j$ for $i \neq j$. So we just need to solve $p^{\alpha - 1}(p - 1) = a$ for $p$ prime and $\alpha$ where $a$ is a factor of 12. Since $12 = 1 \cdot 12$, $12 = 4 \cdot 3$ and $12 = 2 \cdot 6$ are the only possible factorisations, $r$ is at most 2. We are considering any factorisations of 12 since the factors $(p_i - 1)$ are not prime for $p > 2$.

Consider $12 = 1 \cdot 12$. Clearly, $p^{\alpha - 1}(p - 1) = 1$ if and only if $p = 1$ and $\alpha = 1$, and $p^{\alpha - 1}(p - 1) = 12$ if and only if $p = 13$ and $\alpha = 1$. Notice that there is no prime satisfying $p^{\alpha - 1} = 12$ for any $\alpha \in \mathbb{N}$. We have $n = 13$ or $n = 2 \cdot 13 = 26$.

Now consider $12 = 4 \cdot 3$. If $p^{\alpha - 1}(p - 1) = 3$ then $p - 1 = 3, p^{\alpha - 1} = 1$ or $p - 1 = 1, p^{\alpha - 1} = 3$. However, $p = 4$ is not a prime. In the latter case, $p = 2$ but there is no natural number $\alpha$ giving $2^{\alpha - 1} = 3$. So $\phi(n)$ cannot be of the form $\phi(n) = 4 \cdot 3$. 


Finally, consider $12 = 2 \cdot 6$. We need to solve $p^{\alpha-1}(p - 1) = 2$ and $p^{\alpha-1}(p - 1) = 6$. For $p^{\alpha-1}(p - 1) = 2$ we have two solutions:

$$p = 2, \ \alpha = 2, \ \text{or} \ \ p = 3, \ \alpha = 1.$$  

For $p^{\alpha-1}(p - 1) = 6$ we also have two solutions:

$$p = 7, \ \alpha = 1, \ \text{or} \ \ p = 3, \ \alpha = 2$$  

(consider $6 = 6 \cdot 1$ or $6 = 3 \cdot 2$.) Therefore, the possibilities for $n$ are $n = 2^2 \cdot 7 = 28$, $n = 2^2 \cdot 3^2 = 36$ and $n = 3 \cdot 7 = 21$ (we choose $p_1$, $\alpha_1$ from the first group and $p_2$, $\alpha_2$ from the second group). Notice that $n = 3 \cdot 3^2 = 3^3$ is not an answer since $\phi(3^3) = 3^3 - 3^2 = 18$.

c. Since $p$ is odd $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$. For any $x \in \mathbb{Z}_4$, $x^2 \in \{[0]_4, [1]_4\}$. So, $x^2 + y^2 \equiv 1 \mod 4$ for any $x \in [0]_4$ and $y \in [1]_4$. However, there is no possible choices for $x$ and $y$ that could give $x^2 + y^2 \equiv 3 \mod 4$. Therefore, if $p = x^2 + y^2$ then it has to satisfy $p \equiv 1 \mod 4$.  

Question 2. Using the Chinese Remainder Theorem, or otherwise, deduce whether the following systems of linear congruences have a solution. If they do, calculate the solutions.

(i) \(6x \equiv 5 \mod{11}\) and \(3x \equiv 4 \mod{5}\).

(ii) \(x \equiv 2 \mod{21}, 4x \equiv 2 \mod{18}\) and \(2x \equiv 3 \mod{7}\).

Solution.

(i) First bring the congruences into the form \(x \equiv a \mod{n}\). So, multiply them by the inverse of \(6\) mod \(11\) and the inverse of \(3\) mod \(5\), respectively. We have \([6]_{11}^{-1} = 2, [3]_{5}^{-1} = 2\). Then

\[
\begin{align*}
6x & \equiv 5 \mod{11} \\
2 \cdot 6x & \equiv 2 \cdot 5 \mod{11} \\
x & \equiv 10 \mod{11}
\end{align*}
\]

and

\[
\begin{align*}
3x & \equiv 4 \mod{5} \\
2 \cdot 3x & \equiv 2 \cdot 4 \mod{5} \\
x & \equiv 8 \mod{5} \\
x & \equiv 3 \mod{5}.
\end{align*}
\]

Notice that \((11, 5) = 1\). By the theorem, there exists a unique solution to the system \(\mod{5 \cdot 11 = 55}\). Let us calculate the solution. If \(x\) is a solution to the first congruence then \(x = 11k + 10\) for some \(k \in \mathbb{Z}\). If \(x\) is also a solution to the second one, then

\[x = 11k + 10 \equiv 1 \cdot k + 0 \equiv k \equiv 3 \mod{5}.
\]

So, \(k = 5m + 3\) for some \(m \in \mathbb{Z}\). This gives \(x = 11(5m + 3) + 10 = 55m + 43\). Therefore \([43]_{55}\) is the unique solution.

(ii) We apply the theorem to \(x \equiv 2 \mod{21}\) and \(2x \equiv 3 \mod{7}\). Again, we need to bring the latter into the form \(x \equiv a \mod{7}\) for some \(a \in \mathbb{Z}\). So multiply the both sides by \([2]_{7}^{-1} = [4]_{7}\) to get

\[
\begin{align*}
2x & \equiv 3 \mod{7} \\
4 \cdot 2x & \equiv 4 \cdot 3 \mod{7} \\
x & \equiv 12 \mod{7} \\
x & \equiv 5 \mod{7}.
\end{align*}
\]

Now, by the Chinese Remainder Theorem, \("x \equiv 2 \mod{21}, x \equiv 5 \mod{7}"\) have a common solution if and only if \((21, 7) = 1\). Since this is not the case, there is no common solution satisfying the two congruences. Therefore, there cannot be a common solution to \("x \equiv 2 \mod{21}, 4x \equiv 2 \mod{18}, 2x \equiv 3 \mod{7}"\).
Question 3. Let $a \in \mathbb{Z}^+$. Show that for any integer $n \geq 1$,

\[
\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^n = \begin{pmatrix} a^n & na^{n-1} \\ 0 & a^n \end{pmatrix}.
\]

Solution.

For $n = 1$, we have

\[
\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^1 = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}.
\]

Assume that the equality holds for $n = k$. For $n = k + 1$ we have

\[
\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^{k+1} = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}^k \cdot \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^k & na^{k-1} \\ 0 & a^k \end{pmatrix} \cdot \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{k+1} & (k+1)a^k \\ 0 & a^{k+1} \end{pmatrix}.
\]

Therefore the equality is true for all $n \geq 1$ by the induction principle. □
**Question 4.** A public key code has base 69 and exponent 15. It uses the following letter-to-number equivalents.

- B = 1, G = 2, L = 3, A = 4, E = 5, S = 6, “ ” = 7, T = 8, R = 0.

(Note that 7 corresponds to the “space” character.) A message has been converted to numbers and broken into 2-digits blocks. The coded message is 34/16/28/47. Decode the message.

**Solution.**

We have \( n = 69 = 3 \cdot 23 \). So, \( \phi(69) = (3-1)(23-1) = 44 \). Notice that \((44, 15) = 1\).

We calculate the other integer \( x \) by the formula

\[
x = x \cdot 15 + s \cdot 44
\]

where \( s \in \mathbb{Z} \). We find \( x = 3 \) since

\[
1 = 3 \cdot 15 - 44.
\]

Let us decode 34/16/28/47. We find \( \beta_1/\beta_2/\beta_3/\beta_4 \) by

\[
\begin{align*}
\beta_1 &= 34^3 \text{ mod } 69 \equiv 52 \cdot 34 \equiv 43 \text{ mod } 69, \\
\beta_2 &= 16^3 \text{ mod } 69 \equiv 49 \cdot 16 \equiv 25 \text{ mod } 69, \\
\beta_3 &= 28^3 \text{ mod } 69 \equiv 25 \cdot 28 \equiv 10 \text{ mod } 69, \\
\beta_4 &= 47^3 \text{ mod } 69 \equiv 1 \cdot 47 \equiv 47 \text{ mod } 69.
\end{align*}
\]

Hence, the coded message is 43/25/10/47 which translates into “ALGEBRA ”. \( \square \)
Question 5. Let $A$, $B$ and $C$ be nonempty sets. Prove the following two equalities.

(i) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$,

(ii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$,

Solution.

(i) We use the equality $A \setminus B = A \cap B^c$ and the properties of the set operations \( \cap, \cup \text{ and } " \in " \) to get

\[
(A \setminus B) \cup (B \setminus A) = (A \cap B^c) \cup (B \cap A^c)
\]

\[
= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c]
\]

\[
= [(A \cup B) \cap (B^c \cup B)] \cap [(A \cup A^c) \cap (A^c \cup B^c)]
\]

\[
= (A \cup B) \cap (A^c \cup B^c)
\]

\[
= (A \cup B) \cap (A \cap B)^c
\]

\[
= (A \cup B) \setminus (B \cap A).
\]

Alternatively, we can use the definitions.

$x \in (A \setminus B) \cup (B \setminus A) \implies x \in A \setminus B \text{ or } x \in B \setminus A$

\[
\implies \text{“} x \in A \text{ and } x \notin B \text{” or “} x \in B \text{ and } x \notin A \text{”}
\]

\[
\implies \text{“} x \in A \text{ or } x \in B \text{” and “} x \notin A \text{ or } x \notin B \text{” and}
\]

\[
\text{“} x \in A \text{ or } x \notin A \text{” and “} x \in B \text{ or } x \notin B \text{”}
\]

\[
\implies \text{“} x \in A \text{ or } x \in B \text{” and “} x \notin A \text{ or } x \notin B \text{”}
\]

\[
\implies \text{“} x \in A \cup B \text{” and “} x \notin A \cap B \text{”}
\]

\[
\implies x \in (A \cup B) \setminus (A \cap B).
\]

Note that both “$x \in A$ or $x \notin A$” and “$x \in B$ or $x \notin B$” implies $x \in U$ and that does not effect the claim. Hence, $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (B \cap A)$.

Now assume that $x \in (A \cup B) \setminus (B \cap A)$. Then

$x \in (A \cup B) \setminus (B \cap A) \implies x \in A \cup B \text{ and } x \notin A \cap B$

\[
\implies \text{“} x \in A \text{ or } x \in B \text{” and “} x \notin A \text{ or } x \notin B \text{”}
\]

\[
\implies \text{“} x \in A \text{ and } x \notin A \text{” or “} x \in A \text{ and } x \notin B \text{” or}
\]

\[
\text{“} x \in B \text{ and } x \notin B \text{” or “} x \in B \text{ and } x \notin A \text{”}
\]

\[
\implies \text{“} x \in A \text{ and } x \notin B \text{” or “} x \in B \text{ and } x \notin A \text{”}
\]

\[
\implies x \in A \setminus B \text{ or } x \in B \setminus A.
\]

Note that both “$x \in A$ and $x \notin A$” and “$x \in B$ and $x \notin B$” imply $x \in \emptyset$ and that does not effect the claim. Hence $(A \cup B) \setminus (B \cap A) \subseteq A \setminus B \text{ or } x \in B \setminus A$. Thus, $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (B \cap A)$. 

(ii) Similarly,

\[
A \setminus (B \setminus C) = A \cap (B \setminus C)^c \\
= A \cap (B \cap C)^c \\
= A \cap (B^c \cup (C^c)^c) \\
= A \cap (B^c \cup C) \\
= (A \cap B^c) \cup (A \cap C) \\
= (A \setminus B) \cup (A \cap C).
\]