COMP 2711 Discrete Math Tools for Computer Science

2022 Fall Semester - Homework 4

Question 1: Answer the questions below:

(a) Find all positive integers n such that $n^2 + 1$is divisible by $n + 1$.

(b) Find all integers $x \neq 1$ such that $x - 1 \mid x^3 - 3$.

(c) Prove that if for integers a and b we have $7 \mid a^2 + b^2$, then $7 \mid a$ and $7 \mid b$

(d) Prove that if for some integers a, b, c, we have $9 \mid a^3 + b^3 + c^3$, then at least one of the numbers a, b, c is divisible by 3.

(e) Prove that if for integer a and b the congruence $ax + b = 0 (\text{mod } m)$ has a solution for every positive integer modulus m, then the equation $ax + b = 0$ has an integer solution.

Answer:

(a) $n^2+1 = n^2-1+2 = (n+1)(n-1)+2 \equiv 2(\text{mod } n+1)$. Thus, $\frac{2}{n+1}$ is an integer. Which means $n = 1$.

(b) $x^3 - 3 = x^3 - 1^3 - 2 = (x-1)(x^2 + x + 1) - 2 \equiv -2(\text{mod } x-1)$. Thus, $\frac{-2}{x-1}$ is an integer. Which means $x - 1 \in \{-2, -1, 1, 2\} \to x \in \{-1, 0, 2, 3\}$. (Because we change the question, answer without 3 is acceptable)

(c) Given $7 \mid a^2 + b^2 \to a^2 + b^2 \equiv 0(\text{mod } 7)$, we want to prove that $a \equiv b \equiv 0(\text{mod } 7) \leftrightarrow 7 \mid a$ and $7 \mid b$
We can only consider $a \equiv 0, \pm1, \pm2, \pm3(\text{mod } 7)$. Thus, $a^2 \equiv 0, 1, 4, 9(\text{mod } 7)$, in other words, $a^2 \equiv 0, 1, 4, -2(\text{mod } 7)$. Similarly, $b^2 \equiv 0, 1, 4, -2(\text{mod } 7)$. However, since $a^2 + b^2 \equiv 0(\text{mod } 7) \to b^2 \equiv -a^2(\text{mod } 7)$, $b^2 \equiv 0, -1, -4, 2(\text{mod } 7)$. Therefore, $b^2 \equiv 0(\text{mod } 7)$, which means $b \equiv 0(\text{mod } 7)$. Similarly, $a \equiv 0(\text{mod } 7)$.

(d) Assume that none of a, b, c is divisible by 3, which means that $a, b, c \equiv 1, 2 \equiv \pm1(\text{mod } 3)$. Thus $a^3, b^3, c^3 \equiv \pm1(\text{mod } 3) \leftrightarrow a^3 + b^3 + c^3 \equiv \pm1, \pm3(\text{mod } 3) \to a^3 + b^3 + c^3 \not\equiv 0(\text{mod } 3)$.
However, $9 \mid a^3 + b^3 + c^3 \leftrightarrow a^3 + b^3 + c^3 \text{mod } 9 = 0$. From the lecture note, $a^3 + b^3 + c^3 \text{mod } 3 = (a^3 + b^3 + c^3 \text{mod } 3 \cdot 3) \text{mod } 3 = (a^3 + b^3 + c^3 \text{mod } 9) \text{mod } 3 = 0 \text{mod } 3 = 0$, which means that $a^3 + b^3 + c^3 \equiv 0(\text{mod } 3)$ contradiction.

(e) To prove $ax + b = 0$ has an integer solution, it suffices to prove $a \mid b$. To prove that by contradiction, we assume that $a \nmid b$. Thus we have $b = aq+r$ for some integer q and $0 < r < a$. The congruence becomes $ax + aq + r \equiv 0(\text{mod } m)$. When $m = a$, the congruence doesn't have any solution. This contradicts the given condition.

Question 2: Solve each of these congruences. Please write down the process of finding multiplicative inverses. If you just write down the answer, you will get 0 point even if the answer is correct.

(a) $2011x \equiv 123 (\text{mod } 2711)$

(b) $3675x \equiv 291 (\text{mod } 4409)$

(c) $777x \equiv 896 (\text{mod } 2311)$

Answer: (a) We find the inverse of 2011 modulo 2711 below:
By Extended GCD Algorithm,

$$
\begin{aligned}
2711 &= 2011 \cdot 1 + 700 \\
2011 &= 700 \cdot 2 + 611 \\
700 &= 611 \cdot 1 + 89 \\
611 &= 89 \cdot 6 + 77 \\
89 &= 77 \cdot 1 + 12 \\
77 &= 12 \cdot 6 + 5 \\
12 &= 5 \cdot 2 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}
$$

$\gcd(2011, 2711) = 1$, thus, 2011 has a unique inverse in $\mathbf{Z_{2711}}$.
Rewriting:

$$
\begin{aligned}
700 &= 2711 - 2011 \cdot 1 \\
611 &= 2011 - 700 \cdot 2 \\
89 &= 700 - 611 \cdot 1 \\
77 &= 611 - 89 \cdot 6 \\
12 &= 89 - 77 \cdot 1 \\
5 &= 77 - 12 \cdot 6 \\
2 &= 12 - 5 \cdot 2 \\
1 &= 5 - 2 \cdot 2
\end{aligned}
$$

Substituting:

$$
\begin{aligned}
1 &= 5 - (12 - 5 \cdot 2) \cdot 2 \\
&= 5 \cdot 5 - 12 \cdot 2 \\
&= (77 - 12 \cdot 6) \cdot 5 - 12 \cdot 2 \\
&= 77 \cdot 5 - 12 \cdot 32 \\
&= 77 \cdot 5 - (89 - 77 \cdot 1) \cdot 32 \\
&= 77 \cdot 37 - 89 \cdot 32 \\
&= (611 - 89 \cdot 6) \cdot 37 - 89 \cdot 32 \\
&= 611 \cdot 37 - 89 \cdot 254 \\
&= 611 \cdot 37 - (700 - 611 \cdot 1) \cdot 254 \\
&= 611 \cdot 291 - 700 \cdot 254 \\
&= (2011 - 700 \cdot 2) \cdot 291 - 700 \cdot 254 \\
&= 2011 \cdot 291 - 700 \cdot 836 \\
&= 2011 \cdot 291 - (2711 - 2011 \cdot 1) \cdot 836 \\
&= 2011 \cdot 1127 - 2711 \cdot 836
\end{aligned}
$$

Therefore the inverse of 2011 in $\mathbf{Z_{2711}}$ is $1127 \bmod 2711 = 1127$.
$x \equiv 2011 \cdot 1127 \equiv 123 \cdot 1127 \equiv 360 \pmod{2711}$

(b) The inverse of 3675 in $\mathbf{Z_{4409}}$ is 883.
$x \equiv 3675 \cdot 883 \equiv 291 \cdot 883 \equiv 1231 \pmod{4409}$

(c) The inverse of 777 in $\mathbf{Z_{2311}}$ is 809.
$x \equiv 777 \cdot 809 \equiv 896 \cdot 809 \equiv 1521 \pmod{2311}$

Question 3: Solve this system of linear congruences. If you just write down the answer, you will get 0 point even if the answer is correct.

$$x \equiv 2 (\text{mod } 7)$$
$$x \equiv 3 (\text{mod } 17)$$
$$x \equiv 15 (\text{mod } 23)$$
$$x \equiv 14 (\text{mod } 27)$$

Answer: $m_1 = 7, m_2 = 17, m_3 = 23, m_4 = 27$. $m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 73899$
$M_1 = m/m_1 = 10557$, $M_2 = m/m_2 = 4347$, $M_3 = m/m_3 = 3213$, $M_4 = m/m_4 = 2737$
$10557y_1 \equiv y_1 \equiv 1(\text{mod } 7) \rightarrow y_1 = 1$
$4347y_2 \equiv 12y_2 \equiv 1(\text{mod } 17) \rightarrow y_2 = 10$
$3213y_2 \equiv 16y_2 \equiv 1(\text{mod } 23) \rightarrow y_3 = 13$
$2737y_2 \equiv 10y_2 \equiv 1(\text{mod } 27) \rightarrow y_4 = 19$
$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 = 2 \cdot 10557 \cdot 1 + 3 \cdot 4347 \cdot 10 + 15 \cdot 3213 \cdot 13 + 14 \cdot 2737 \cdot 19 = 1506101$. $x \bmod 73899 = 28121$. So $x = 28121$ is the answer.

Question 4: Consider the following simplified version of the RSA algorithm for public cryptography:

(i) Bob's public key is a pair (n, e), where n is a prime number and e is a positive integer that is smaller than n and is relatively prime with $n - 1$

(ii) Bob's private key is $d = e^{-1} \text{mod } (n - 1)$.

(iii) Alice encrypts a message $m (0 < m < n - 1)$ by calculating $c = m^e \text{mod } n$, and sends the ciphertext c to Bob.

(iv) Bob decrypts the ciphertext c by calculating $c^d \text{mod } n$.

Suppose $n = 251$ and $e = 137$.

(a) Calculate d using the extended GCD algorithm. Show the computational steps.

(b) Suppose $m = 200$. Calculate $c = m^e \text{mod } n$ using repeated squaring. Show the computational steps.

(c) Is the system secure? Explain why or why not.

Answer: (a) Note that $n - 1 = 250$ and $e = 137$. We use the extended GCD algorithm.

$$
\begin{aligned}
250 &= 137 \cdot 1 + 113 \\
137 &= 113 \cdot 1 + 24 \\
113 &= 24 \cdot 4 + 17 \\
24 &= 17 \cdot 1 + 7 \\
17 &= 7 \cdot 2 + 3 \\
7 &= 3 \cdot 2 + 1 \\
3 &= 1 \cdot 3 + 0
\end{aligned}
$$

So, $\gcd(250, 137) = 1$. Thus, 250 and 137 are relatively prime.
Rewriting:

$$
\begin{aligned}
113 &= 250 - 137 \cdot 1 \\
24 &= 137 - 113 \cdot 1 \\
17 &= 113 - 24 \cdot 4 \\
7 &= 24 - 17 \cdot 1 \\
3 &= 17 - 7 \cdot 2 \\
1 &= 7 - 3 \cdot 2
\end{aligned}
$$

Substituting:

$$\begin{aligned}
1 &= 7 - (17 - 7 \cdot 2) \cdot 2 \\
&= 7 \cdot 5 - 17 \cdot 2 \\
&= (24 - 17 \cdot 1) \cdot 5 - 17 \cdot 2 \\
&= 24 \cdot 5 - 17 \cdot 7 \\
&= 24 \cdot 5 - (113 - 24 \cdot 4) \cdot 7 \\
&= 24 \cdot 33 - 113 \cdot 7 \\
&= (137 - 113 \cdot 1) \cdot 33 - 113 \cdot 7 \\
&= 137 \cdot 33 - 113 \cdot 40 \\
&= 137 \cdot 33 - (250 - 137 \cdot 1) \cdot 40 \\
&= 137 \cdot 73 - 250 \cdot -40
\end{aligned}$$

Therefore the inverse of 137 in $\mathbf{Z_{250}}$ is $73 \bmod 250 = 73$.
Thus, $d = 73$.

(b)

$$\begin{aligned}
200^{2^0} \bmod 251 &= 200 \\
200^{2^1} \bmod 251 &= 200^2 \bmod 251 = 91 \\
200^{2^2} \bmod 251 &= 91^2 \bmod 251 = 249 \\
200^{2^3} \bmod 251 &= 249^2 \bmod 251 = 4 \\
200^{2^4} \bmod 251 &= 4^2 \bmod 251 = 16 \\
200^{2^5} \bmod 251 &= 16^2 \bmod 251 = 5 \\
200^{2^6} \bmod 251 &= 5^2 \bmod 251 = 25 \\
200^{2^7} \bmod 251 &= 25^2 \bmod 251 = 123
\end{aligned}$$

Note that $137 = 2^0 + 2^3 + 2^7$.
Therefore, $200^1 37 \equiv 200^{2^0} \cdot 200^{2^3} \cdot 200^{2^7} \equiv 200 \cdot 4 \cdot 123 \equiv 8 (\bmod 251)$.

(c) No. The system is not secure. As the public key is (n, e), the attacker could compute $n - 1$ from n, then compute d as the inverse of e in $\mathbf{Z_{n-1}}$.