**Name**——————————————————————————, **ID** ——————————

 

# HW II

Ayman Badawi

**QUESTION 1.** Let $A = \begin{bmatrix} 2 & 5 \\ 1 & 1 \end{bmatrix}$. Find $A^{-1}$ over $Z_{16}$ if possible.

(**HINT: note that** $\begin{vmatrix} 2 & 5 \\ 1 & 1 \end{vmatrix} \ (mod\ 16) = -3 \ (mod\ 16) = 13$**. Since** $gcd(13, 16) = 1$**,** $A^{-1}$ **exists over** $Z_{16}$ **by class notes. Thus** $A^{-1} = 13^{-1} \begin{bmatrix} 1 & -5 \\ -1 & 2 \end{bmatrix} = 5 \begin{bmatrix} 1 & 11 \\ 15 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 11 & 10 \end{bmatrix} \ in\ Z_{16}$)

**QUESTION 2.** Let $A = \begin{bmatrix} 2 & 6 \\ 1 & 1 \end{bmatrix}$. Find $A^{-1}$ over $Z_{18}$ if possible.

(**HINT: note that** $\begin{vmatrix} 2 & 6 \\ 1 & 1 \end{vmatrix} \ (mod\ 18) = -4 \ (mod\ 18) = 14$**. Since** $gcd(14, 18) \neq 1$**,** $A^{-1}$ **does not exists over** $Z_{18}$)

**QUESTION 3.** Solve the following system of L.E. over $Z_{12}$.

$$2x_1 + 7x_2 + 4x_3 = 2$$

$$x_1 + x_2 + 5x_3 = 7$$

$$x_1 + 4x_3 = 1$$

(**HINT: Find the determinant of the coefficient matrix, I guess it will be 11, Use Cramer, for example find** $x_1, x_3$**, then by substitution find** $x_2$**, note** $11^{-1} = 11 \ in \ Z_{12}$**. See class notes** )

**QUESTION 4.** Let $d = gcd(660, 385)$. Find $c_1, c_2$ such that $d = 660n_1 + 385n_2$

(**HINT: See class notes for exam-one**)

**QUESTION 5.** Let $p$ be a prime number such that $2^p - 1$ is prime. Prove that $2^{(p-1)}(2^p - 1)$ is a perfect even integer.

(**HINT: See class notes for exam-one**)

**QUESTION 6.** (a) Find the quadratic residue (i.e., square residue) of $Z_{23}^*$

(**HINT: Since** $5^{(p-1)/2} = 5^{22/2} = 5^{11} = 22$**, 5 is a generator of** $Z_{23}^*$**, i.e,** $Z_{23}^* = \{5, 5^2, ..., 5^{22} = 1\}$**. Hence by class notes,** $QR(23) = SR(23) = \{5^i \mid i$ **is EVEN and** $2 \leq i \leq 22\} = \{5^2, 5^4, 5^6, 5^8, 5^{10}, 5^{12}, 5^{14}, 5^{16}, 5^{18}, 5^{20}, 5^{22} = 1\} = \{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1\}$**. Note that as expected,** $|QR(23) = |SR(23)| = 11$**.** )

(b) Find the solution set of $x^2 = 6$ in $Z_{23}$

(**HINT: By staring, we observe** $6 \in QR(23) = SR(23)$**. By staring,** $5^{18} = (5^9)^2 = 6$ **in** $Z_{23}$**. Hence** $x_1 = 5^9 \ (mod\ 23) = 11$**, and** $x_2 = 23 - 11 = 12$**. Solution set is** $\{11, 12\}$ )

(c) Find all integers in $Z$, say $y$, such that $y^2 \ (mod\ 23) = 6$

(**HINT: In view of (b), the solution set over** $Z$ **is** $\{11 + 23k \mid k \in Z\} \cup \{12 + 23m \mid m \in Z\}$**. Note** $\{11 + 23k \mid k \in Z\} \cap \{12 + 23m \mid m \in Z\} = \emptyset$ )

(d) Find the solution set of $x^2 = 5$ in $Z_{23}$.

(**HINT: By staring, we observe** $5 \notin QR(23) = SR(23)$**. Hence the solution set is** $\{\} = \phi$)

**QUESTION 7.** Find All ordered pairs $(x, y)$ over $Z_7$. Such that $3x^2 + y^2 = 5$ in $Z_7$ (note that 0 is allowed here)

(**HINT: All possible values of** $x^2$ **in** $Z_7$ **are the** $SR(7) \cup \{0\} = QR(7) \cup \{0\} = \{0, 1, 4, 2\}$**. Hence all possible values of** $3x^2$ **in** $Z_7$ **are** $\{0, 3, 5, 6\}$**.**
**All possible values of** $y^2$ **in** $Z_7$ **are the** $SR(7) \cup \{0\} = QR(7) \cup \{0\} = \{0, 1, 4, 2\}$**.**
**Hence all ordered pairs** $(3x^2, y^2)$ **such that** $3x^2 + y^2 = 5$ **are** $(3, 2), (5, 0)$
**(i) Now for** $(3, 2)$**, we have** $x^2 = 1$ **and** $y^2 = 2$**. Hence** $x \in \{1, 6\}$ **and** $y \in \{3, 4\}$**.**
**(ii) For** $(5, 0)$**, we have** $x^2 = 4$ **and** $y^2 = 0$**. Hence** $x \in \{2, 5\}$ **and** $y \in \{0\}$**.**
**(iii) Thus (i) and (ii) imply that all ordered pairs** $(x, y)$ **over** $Z_7$ **are** $\{(1, 3), (1, 4), (6, 3), (6, 4), (2, 0), (5, 0)\}$ )

**QUESTION 8.** Find All ordered pairs $(x, y)$ over $Z$ Such that $3x^2 + y^2 \pmod 7 = 5$

(**HINT: By staring at (iii) in Question 7, all ordered pairs** $(x, y)$ **over** $Z$ **Such that** $3x^2 + y^2 \pmod 7 = 5$ **are** $\{(1+7n_1, 3+7m_1), (1+7n_2, 4+7m_2), (6+7n_3, 3+7m_3), (6+7n_4, 4+7m_4), (2+7n_5, 7m_5), (5+7n_6, 7m_6) \mid n_1, ..., n_6 \in Z; m_1, ..., m_6 \in Z\}$ )

**QUESTION 9.** Let $p \geq 2$ be a prime integer and $m \geq 2$ be an integer such that $gcd(m, p-1) = 1$. Then the m-residue of $Z_p$, call it $m - R(p)$, is $Z_p^*$, and $x^m = a$ has exactly one solution in $Z_p^*$ for every $a \in Z_p^*$.

(**HINT: See class notes**)

**QUESTION 10.** Prove that there are infinitely prime integers of the form $4k + 3$.(see class notes)

**QUESTION 11.** (a) Important, Let $a \in k - R(p)$, $a \neq 0$, such that $k \mid (p-1)$. Then $x^k = a$ has exactly $k$ solutions in $Z_p^*$. How do you find them? **Solution: Let** $w$ **be a generator of** $Z_p^*$**,** $m = (p-1)/k$**,** $f = w^k$**. Then** $k - R(P) = \{f, f^2, ..., f^m = 1\}$ **and** $|k - R(p)| = m$**. Find the unique subset (subgroup) of** $Z_p^*$ **with k elements, say C(k), where** $d^k = 1$ **for every** $d \in C(k)$**. Let** $h = w^m$**. Then** $C(k) = \{h, h^2, ..., h^k = 1\}$ **Since** $a \in k - R(p)$**,** $a = f^i = (w^k)^i = (w^i)^k$**. Then** $w^i$ **is a solution to the equation** $x^k = a$**. Now the solution set to the equation** $x^k = a$ **is** $w^i C(k) = \{w^i h, w^i h^2, ..., w^i h^k\}$ )

(b) Use (a) above, find the solution set to $x^3 = 5$ and to $y^4 = 3$ over $Z_{13}$.

(c) Find all ordered pairs $(x, y)$ over $Z_{13}$ such that $x^3 + y^4 = 8$

(d) Find all ordered pairs $(x, y)$ over $Z$ such that $x^3 + y^4 \pmod{13} = 8$.

(e) Assume $p - 1 = km$. From (a), observe this interesting result: assume that $a \in k - R(p)$. Assume $b^k = a$. Then the solution set to $x^k = a$ is $b * (m - R(p))$

**QUESTION 12.** Find $x, y \in Z$ such that $(100 + 81)^2 = x^2 + y^2$

**QUESTION 13.** Which of the following numbers are in $5 - R(41)$?
10, 7, 9, 17, 14, 22, 27.

(**see class notes, I guess you need to check if** $a^8 = 1$ **in** $Z_{41}$ )

**QUESTION 14.** (a) Let $a$ be a positive integer. Prove that there is a right triangle with $a^2 + (a+1)^2$ as the hypotenuse.

(b) Assume that $a, b$ are positive integer such that $a^2 + b^2 = c$ for some odd integer $c$. Prove that $c \pmod 4 = 1$. (Hint: you may assume that a is even and b is odd)

(c) Prove that none of the numbers 19, 23, 35 is a sum of two squares (Hint: see (b))

**QUESTION 15.** Let $a > b > 1$, $a, b \in Z$. Assume that $gcd(a, b) = 1, ab = x^2$ for some $x \in Z$. Show that $a = y^2, b = w^2$ for some $y, w \in Z$. (see class notes)

**QUESTION 16.** Given 56 is the length of a leg of a primitive right triangle that has the maximum area possible. Assume that the length of each side is an integer. What is the area of such triangle? What is the length of the hypotenuse of such triangle? (See class notes)

**QUESTION 17.** Let $x > y > 1$ be odd integers such that $x^2 - y^2 = 4m^2$ for some integer $m > 1$. Prove that $m$ is an even integer. (This will convince you that if 2ab is a leg of a primitive right triangle, then ab is an even integer, see class note)

**QUESTION 18.** (a) Convince me that there is only one primitive right triangle with a leg of length 64, where the length of each side is an integer. (see class notes, scratch ur forehead a little)

(b) Give me three distinct primitive right triangles, where each side has an integer length and all three share a leg of length 60.

**QUESTION 19.** Prove that there is no integer solutions for $x^2 - y^2 = 42$. (See class notes: $(x^2 - y^2)\ (mod\ 4) = 0$, but 42 (mod 4) = 2.)

### Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com