Name Joud Hamdan , ID 95608

36/36

Final Exam

Ayman Badawi

QUESTION 1. (i) Find the quadratic residue (i.e., square residue) of Z_{19}^*.

$a^9 = 18$ in Z_{19}^*

$a = 2$

$QR(19) = \{2^2, (2^2)^2, (2^2)^3, (2^2)^4, (2^2)^5, (2^2)^6, (2^2)^7, (2^2)^8, (2^2)^9\}$

$= \{4, 16, 7, 9, 17, 11, 6, 5, 1\}$

(ii) Find the solution set of $x^6 = 11$ in Z_{19}.

By staring at (i), one solution is $2^2 = 4$

$C(6) = \{2^3, (2^3)^2, (2^3)^3, (2^3)^4, (2^3)^5, (2^3)^6\}$

$= \{8, 7, 18, 11, 12, 1\}$

Solution set is $4C(6) = \{13, 9, 15, 6, 10, 4\}$

(iii) Find all integers in Z, say y, such that $y^2 \pmod{19} = 6$.

By (i), one solution is $2^7 = 14$

Other solution is $19 - 14 = 5$

Solution over Z is $\{14 + 19k_1, 5 + 19k_2 \mid k_1, k_2 \in Z\}$

QUESTION 2. Prove that there are infinitely prime integers of the form $4k+3$.

Deny. $\exists$ finitely many prime integers of the form $4k+3$, say $p_1, p_2, \ldots, p_k$. Let $x = 4p_1p_2 \ldots p_k - 1$ $(*)$

$x = q_1 q_2 \ldots q_m$ (prime factorization) $(**)$

Each q_i, $1 \le i \le m$, is a factor of x but each p_i, $1 \le i \le k$ is never a factor of x. Thus each q_i must be of the form $4k+1$. By $(**)$, $x \pmod 4) = q_1 q_2 \ldots q_m \pmod 4) = 1$, but by $(*)$ $x \pmod 4) = -1 \pmod 4) = 3$, a contradiction

QUESTION 3. 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 $y, w \in Z$.

$x = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ (prime factorization)

$x^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots p_k^{2\alpha_k} = ab$. Since $gcd(a,b) = 1$. Then each $p_i^{2\alpha_i}$ is either a factor of a or b. $a = q_1^{2\alpha_1'} q_2^{2\alpha_2'} \ldots q_m^{2\alpha_m'}$ where $q_1^{2\alpha_1'}, q_2^{2\alpha_2'}, \ldots, q_m^{2\alpha_m'} \in \{p_1^{2\alpha_1}, p_2^{2\alpha_2}, \ldots, p_k^{2\alpha_k}\}$.

$b = s_1^{2\alpha_1''} s_2^{2\alpha_2''} \ldots s_n^{2\alpha_n''}$ where $s_1^{2\alpha_1''}, s_2^{2\alpha_2''}, \ldots, s_n^{2\alpha_n''} \in \{p_1^{2\alpha_1}, p_2^{2\alpha_2}, \ldots, p_k^{2\alpha_k}\} - \{q_1^{2\alpha_1'}, \ldots, q_m^{2\alpha_m'}\}$. Thus we have shown that $a = (q_1^{\alpha_1'} q_2^{\alpha_2'} \ldots q_m^{\alpha_m'})^2$ and $b = (s_1^{\alpha_1''} s_2^{\alpha_2''} \ldots s_n^{\alpha_n''})^2$

QUESTION 4. Let $n, m \ge 1$ be positive integers and $x \in Z^+$. Show that $3^n + 3^m + 1 \ne x^2$.

Let $k \in Z^+$. $3^{2k} \pmod 8) = (9^k) \pmod 8) = 1$

$3^{2k+1} \pmod 8) = 3^{2k} \cdot 3 \pmod 8) = 1 \cdot 3 = 3$.

We conclude $\forall\, k \in Z^+$, $3^k \pmod 8) = \{1, 3\}$. Thus possibilities for $(3^n + 3^m + 1) \pmod 8) = \{3, 5, 7\}$, but $x^2 \pmod 8) = \{0, 1, 4\}$

Since $\{3,5,7\} \cap \{0,1,4\} = \emptyset$,

$3^n + 3^m + 1 \ne x^2 \;\forall\, n, m, x \in Z^+$.

QUESTION 5. Find all positive prime integers, say p, such that $p \mid (459^p + 1)$.

Claim: $\gcd(459, p) = 1$. Suppose not. Then $p \mid 459$, but since $p \mid (459^p + 1)$ then $p \mid 1$, a contradiction. Thus $\gcd(459, p) = 1$ and we can use Euler. $459^{p-1} \pmod p = 1 \Rightarrow 459^p \pmod p = 459 \pmod p$

$459^p + 1 \pmod p = 460 \pmod p$. Since $p \mid (459^p + 1)$, then

$p \mid 460 \Rightarrow p = 2, 5, 23$

QUESTION 6. Let $m > 1$ be an integer and $f(n) = n^m + a_{m-1}n^{m-1} + \ldots + a_1 n + a_0$, where all the $a_i's$ are integers and $n \in Z$. Given $f(b_1) = f(b_2) = f(b_3) = 22$ for some distinct $b_1, b_2, b_3 \in Z$. Prove that $f(k) \neq 25$ for every $k \in Z$.

Let $h(n) = f(n) - 22$. Then $h(b_1) = h(b_2) = h(b_3) = h(b_4) = 0$

Then $h(n) = (n-b_1)(n-b_2)(n-b_3)(n-b_4)d(n)$. Assume $f(k) = 25 \; \exists \; k \in Z$.

Then $h(k) = (k-b_1)(k-b_2)(k-b_3)(k-b_4)d(k) = 3$. Max no. of distinct factors for 3 is 3 $((-3)(1)(-1))$ but $|\{k-b_1, k-b_2, k-b_3, k-b_4\}| = 4$ since b_i's are distinct

a contradiction

QUESTION 7. Prove that for each integer $n > 1$, $(2^n - 1)$ is never a factor of $x^2 + 1$ for every $x \in Z$.

Deny. Suppose $2^n - 1 \mid x^2 + 1 \; \exists \; x \in Z$.

$2^n - 1 \pmod 4 = 3$. Let $2^n - 1 = p_1 p_2 \ldots p_k$ (prime factorization)

Then $p_1 p_2 \cdots p_k \pmod 4 = 3$. This means $\exists \; p_i \in \{p_1, p_2, \ldots, p_k\}$ s.t. p_i is of the form $4k+3$. Since $p_i \mid 2^n - 1 \mid x^2 + 1 \Rightarrow p_i \mid x^2 + 1$

$\therefore x^2 \pmod{p_i} = p_i - 1 \Rightarrow x^2 = p_i - 1$ in Z_{p_i}. $p_i - 1 \in SR(p_i)$

but $4 \nmid p_i - 1 = 4k + 2$, a contradiction