Name Furqan Sajjad, ID 94983

~~57~~ 58
60

Exam II

Ayman Badawi

QUESTION 1. (4 points) 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.

let $n = 2^{p-1}(2^p - 1)$

$$\sum_{d \| n} d = 1 + 2 + 2^2 + \dots + 2^{p-1} + (2^p - 1) + 2(2^p-1) + \dots + 2^{p-2}(2^p-1)$$

$$= \frac{2^p - 1}{2-1} + (2^p - 1)(1 + 2 + \dots + 2^{p-2})$$

ok

$$= (2^p - 1) + (2^p - 1)\left[\frac{2^{p-1} - 1}{2-1}\right] = (2^p - 1)(1 + 2^{p-1} - 1)$$

$$= (2^p - 1)(2^{p-1})$$

$$= n \checkmark$$

QUESTION 2. (4 points) Let $d = gcd(21, 60)$. Find c_1, c_2 such that $d = 21n_1 + 60n_2$

$60 = 2 \cdot 21 + 18$ ($60 - 42 = 18$), $21 = 1 \cdot 18 + 3$ ($21 - 18 = 3$), $18 = 6 \cdot 3 + 0$ ($18 - 18 = 0$)

$gcd(21, 60) = \boxed{3}$

$3 = 21 - 1 \cdot 18$ $\qquad$ $3 = 21 - 1 \cdot 18$

$= 21 - 1(60 - 2 \cdot 21)$

$= 21 - 60 + 2 \cdot 21$

$= 3 \cdot 21 - 1 \cdot 60$

$= 21(3) + 60(-1)$ so $\boxed{n_1 = 3, n_2 = -1}$

ok

QUESTION 3. (4 points) Let $A = \begin{bmatrix} 1 & 7 \\ 1 & 2 \end{bmatrix}$. Find A^{-1} over Z_8 if possible.

$|A| = 2 - 7 = -5 = 3 \pmod 8$

ok

$gcd(|A|, n) = gcd(3, 8) = 1$ so A^{-1} exists over Z_8

$$A^{-1} = \frac{1}{|A|}\begin{bmatrix} d & -b \pmod 8 \\ -c \pmod 8 & a \end{bmatrix} = 3^{-1}\begin{bmatrix} 2 & 1 \\ 7 & 1 \end{bmatrix} = 3\begin{bmatrix} 2 & 1 \\ 7 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 3 \\ 21 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 6 & 3 \\ 5 & 3 \end{bmatrix} \pmod 8$$

QUESTION 4. (4 points) Solve for x_3 only in the following system of L.E. over Z_{10}.

$$3x_1 + 4x_2 + 6x_3 = 2$$

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

$$7x_1 + 6x_2 + 3x_3 = 1$$

coef. matrix = $\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 2 \\ 7 & 6 & 3 \end{bmatrix} = A$

$|A| = 3(3-12) - 4(3-14) + 6(6-7)$
$= 11 = 1 \pmod{10}$

$X_3 = \frac{|A_3|}{|A|} = \frac{7}{1} = \boxed{7}$

$A_3 = \begin{bmatrix} 3 & 4 & 2 \\ 1 & 1 & 7 \\ 7 & 6 & 1 \end{bmatrix}$

$|A_3| = 3(1-42) - 4(1-49) + 2(6-7)$
$= 67 = 7 \pmod{10}$

QUESTION 5. (4 points) Prove that there are infinitely prime integers of the form $4k + 3$

Deny. Say there are a finite number of prime int. of the form $4k+3$ and call them $p_1, p_2, \dots, p_m$

let $n = 4p_1p_2 \cdots p_m - 1$ so $n \pmod 4 = -1 = 3 \pmod 4$

The prime factorization of n is $n = q_1 q_2 q_3 \cdots q_\alpha$

We know that none of the p_i's are a factor of n but the q_j's are factors of $n \Rightarrow q_j$ must be of the form $4k+1$,

so n = product of $(4k+1) \Rightarrow n \pmod 4 = 1$ but earlier we said $n \pmod 4 = 3$ ↯

So there are infinitely many prime integers of the form $4k+3$.

QUESTION 6. (Do not use try and error, use mathematical methods as explained in class and HW2)

(i) **(4 points)** Find the quadratic residue or 2-residue of Z_{19}. Note that 2 is a generator of Z_{19}^*.

$QR(19) = \{(2^2)^1, (2^2)^2, (2^2)^3, (2^2)^4, (2^2)^5, (2^2)^6, (2^2)^7, (2^2)^8, (2^2)^9\}$

ok $|QR(19)| = \frac{19-1}{2} = \frac{18}{2} = 9$ $= \{4, 16, 7, 9, 17, 11, 6, 5, 1\}$

(ii) **(4 points)** Find the 3-residue of Z_{19}, i.e., $3 - R(19)$.

$3-R(19) = \{(2^3)^1, (2^3)^2, (2^3)^3, (2^3)^4, (2^3)^5, (2^3)^6\}$

ok $|3-R(19)| = \frac{19-1}{3} = 6$ $= \{8, 7, 18, 11, 12, 1\}$

(iii) **(4 points)** Find the solution set of $x^3 = 7$ in Z_{19}

$7 = (2^3)^2 = (2^2)^3$ so $x = 2^2 = 4 \pmod{19}$ 4, 6, 9

ok (1) let w be a generator of $Z_{19}^* \Rightarrow w = 2$ (2) $k = 3$ $x^3 = 7$ $a = 7$

$a = (w^k)^i \Rightarrow 7 = (2^3)^i = 8^i \pmod{19}$ $m = \frac{p-1}{k} = \frac{18}{3} = 6$

$\Rightarrow i = 2$ is a solution because $7 = 8^i = (2^3)^i$ and we see $i=2$ satisfies from 3-R(1

S.S $= \{w^{i+m}, w^{i+2m}, w^{i…$ $= \{9, 6, 4$

(iv) **(4 points)** Find the solution set of $x^2 = 5$ in Z_{19}

$5 = (2^2)^8 = (2^8)^2 \pmod{19}$

so $x_1 = 2^8 = 9$ & $x_2 = 19 - x_1 = 10$

$S.S = \{9, 10\}$ over Z_{19}

(v) **(4 points)** Find all ordered pairs (x, y) over Z_7 such that $x^3 + y^2 = 5$ in Z_7. Note that 3 is a generator of Z_7^*.

$SR(7) = 2\text{-}R(7) = \{3^2, 3^4, 3^6 = 1\} = \{2, 4, 1\}$

$|SR(7)| = \frac{7-1}{2} = 3$

$3\text{-}R(7) = \{3^3, 3^6 = 1\} = \{6, 1\}$

ok $|3\text{-}R(7)| = \frac{7-1}{3} = 2$

x^3	y^2
0 ×	0
1	1
6	2
	4

$x^3 \in 3\text{-}R(7) \cup \{0\} \Rightarrow x^3 \in \{0, 1, 6\}$

$y^2 \in SR(7) \cup \{0\} \Rightarrow y^2 \in \{0, 1, 2, 4\}$

$\overset{x^3}{(1}, \overset{y^2}{4)}$ is only possible pair

Ordered pairs are $\{(1,2), (1,5), (2,2), (2,5), (4,2), (4,5)\}$ over Z_7

$x^3 = 1 \pmod 7 \Rightarrow x = 1$ or $x = 2$ or $x = 4$

$y^2 = 4 \pmod 7 \Rightarrow y = 2$ or $y = 7 - 2 = 5$

(vi) **(4 points)** Find all ordered pairs (x, y) over Z such that $x^3 + y^2 \ (mod\ 7) = 5$.

$S.S = \{(1+7m_1, 2+7n_1)\} \cup \{(1+7m_2, 5+7n_2)\} \cup \{(2+7m_3, 2+7n_3)\}$
$\cup \{(2+7m_4, 5+7n_4)\} \cup \{(4+7m_5, 2+7n_5)\} \cup \{(4+7m_6, 5+7n_6)\}$

$m_1, \dots, m_6 \in Z$
$n_1, \dots, n_6 \in Z$

OK

(vii) **(4 points)** Which of the following is in $6 - R(31)$: 10, 13, 8, 16

$a \in m\text{-}R(p)$ iff. $a^{\frac{p-1}{gcd(m,p-1)}} = 1 \pmod p$

$p = 31$
$p - 1 = 30$
$m = 6$
$gcd(m, p-1) = 6$

so $a^5 = 1 \pmod{31}$

$10^5 \pmod{31} = 25 \neq 1$ X
$13^5 \pmod{31} = 6 \neq 1$ X
$8^5 \pmod{31} = 1$ ✓
$16^5 \pmod{31} = 1$ ✓

so $8, 16 \in 6\text{-}R(31)$

OK

QUESTION 7. (a) **(4 points)** Given 36 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?

$a^2 + b^2$, $a^2 - b^2$, $2ab = 36$ is even length

$\Rightarrow$ length of hypotenuse $\boxed{325}$, 323, 36

$A = \frac{1}{2}(2ab)(a^2 - b^2)$
$= 18 \cdot 323 = \boxed{5814}$

b^2+c^2, b^2-c^2, $2bc$; $2bc = a^2$

$36 = 2ab \Rightarrow ab = 18$
$= 1 \cdot 18 \longrightarrow$ pair that will give maximum
$= 2 \cdot 9$
$= 3 \cdot 6$

say $a = 18$, $b = 1$

OK

(b) **(4 points)** Let a be an odd positive integer. Can we construct a primitive right triangle such that a^2 is the length of a leg? explain

$u^2 + v^2$, $2uv$, $a^2 = u^2 - v^2$
$u > v \geq 1$

let a be odd
$a = 2k+1$
$a^2 = 4k^2 + 4k + 1$

$2uv$, $u^2 - v^2 = a^2 = 4k^2 + 4k + 1$

let $a = 5$
ex: 13, 12 and 313
possible: $5 = 3^2 - 2^2$, $25 = 13^2 - 12^2$ are both right primitive.

$a^2 = 4k^2 + 4k + 1$
say u is odd, v is even

$u^2 - v^2 = a^2$
$u = \frac{a^2+1}{2}$, $v = \frac{a^2-1}{2}$

4/4

(c) **(4 points)** Let a be an even positive integer. Can we construct a primitive right triangle such that a^2 is the length of a leg? explain

a ~~is even $\Rightarrow$~~ $a = 2m, m \in Z^+$
~~a^2 is even $\Rightarrow a^2 = 4m^2$~~

$u^2 + v^2$, $2uv = a^2$, $u^2 - v^2$

~~If $\frac{a^2}{4} - 1$ is odd~~, then the below will work

$4b^2 = a^2$
$\Rightarrow 4b^2 = 2uv$
$\Rightarrow 4 \cdot 2l = 2uv$
$\Rightarrow 4l = uv$

ex: let $a = 2$; 241, $a^2 = 4$, 15; $4 = 1 \cdot 4 = 2 \cdot 2$

let ~~x~~ $= u^2 + v^2$
$y = u^2 - v^2$
$(2uv)^2$
Then $x^2 - y^2 = 4u^2v^2 = 4b^2$
$\Rightarrow (x-y)(x+y) = 4b^2$
$\Rightarrow 2c \cdot 2d = 4b^2$
$\Rightarrow cd = b^2$

$x - y = 2c$
$x + y = 2d$
~~$2x = 2(c+d)$~~
~~$\Rightarrow x = c + d$~~ so ~~c, d have opp parity~~
odd
cd is even $\Rightarrow b^2$ is even

ex: 265, 3, 16; $a = 4$

$\left(\frac{a^2}{2}\right)^2 + 1$, a^2, $\left(\frac{a^2}{2}\right)^2 - 1$

let a be even
$a = 2k$
$a^2 = 4k^2$
$4k^2 + 1 = u^2 + v^2$
$2uv = a^2 = 4k^2$
$a^2 = 4k^2$
$4k^2 - 1 = u^2 - v^2$
$= 1 \cdot 4k^2$
$= 2 \cdot 2k^2$
$= 4 \cdot k^2$
let $u = 4k^2$, $v = 1$

3/4