Mid Sem II Part II **Discrete Structures - Solution Key** **3x5=15 Marks**

1. Complete the return parameters in the following code for the extneded Euclidian algorithm so that, on input integers $a > b \geq 0$ the algorithm returns the tuple $< d, \alpha, \beta >$ where d =GCD(a, b) and $a\alpha + b\beta = d$, α, β integers. You **must** justify your answer to get *any* credits. $\boxed{3}$

   $< d, \alpha, \beta >$ $Euclid(a, b)$

   if $(a = b)$ return$(a, 1, 0)$ /* return(b,0,1); return(a,0,1); return(b,1,0) also works fine */

   else if $(a < b)$ $< d, \alpha, \beta >=$ $Euclid$(b,a); return $< d, \beta, \alpha >$

   else if $(a > b)$ $< d, \alpha, \beta >=$ $Euclid(a - b, b)$; return $(d, \alpha, \beta - \alpha)$

   The last part follows from $d = \alpha(a - b) + \beta b = \alpha a + (\beta - \alpha)b$.

2. How may numbers between 1 and 5000 (both inclusive) have GCD 4 with 5000? Don't blindly use a formula without justification. (You are allowed to assume the formula for $\phi(m)$ and that the number of integers between 1 and m which are co-prime to m is $\phi(m)$ for any positive integer m). $\boxed{3}$

   $|\{1 \leq i \leq n | GCD(i, n) = d\}| = |\{i \leq j \leq \frac{n}{d} | GCD(j, \frac{n}{d}) = 1\}| = \phi(\frac{n}{d})$. Here $n = 5000, d = 4$. Thus solution is $\phi(1250)$.

3. Consider the linear transformation T in $\mathbf{R^2}$ which maps $[x, y]$ to $[x + y, 0]$. Let $[a, 0] \in \mathbf{R^2}$. What is the inverse image of $(a, 0)$? (That is find the general solution to $T[x, y] = [a, 0]$). $\boxed{3}$

   Nullspace(T)=$\{[x, -x] : x \in \mathbf{R}\}$. $T[a, 0] = [a, 0]$. Hence the general solution is the $[a, 0]$+Nullspace(T). That is $\{[a + x, -x] | x \in \mathbf{R}\}$.

4. Let $p > 2$ be a prime number. How many numbers in $\{0, 1, 2, ..., p-1\}$ satisfy the equation $x^2 - 1 = 0 \mod p$? Justify your answer. $\boxed{3}$

   $x^2 - 1 = 0 \mod p$ if and only if $(x + 1)(x - 1) = 0 \mod p$ if and only if $p|(x + 1)$ or $p|(x - 1)$ (if a prime divides a product, it must divide one of the factors). Since $x \in \{0, 1, 2, ..., p - 1\}$, we have $x \in \{1, p - 1\}$. There are exactly two solutions as $p > 2$.

5. Let $p > 2, q > 2$ be *distinct* prime numbers. How many numbers in $\{0, 1, 2, ..., pq - 1\}$ satisfy the equation $x^2 - 1 = 0 \mod pq$? (Hint: Use previous question and the Chinese remainder theorem). $\boxed{3}$

   To solve $x^2 - 1 = 0$ in $\mathbf{Z}_{pq}$, from Chinese remainder theorem, it follows that it is sufficient to solve the equation in $\mathbf{Z}_p \times \mathbf{Z}_q$. $(a, b) \in \mathbf{Z}_p \times \mathbf{Z}_q$ is a solution to $x^2 - 1 = 0$ if and only if $(a^2, b^2) = 1$. This requires $a^2 = 1$ in $\mathbf{Z}_p$ as well as $b^2 = 1$ in $\mathbf{Z}_q$ Thus $a \in \{1, p-1\}$ in $\mathbf{Z}_p$ and $b \in \{1, q-1\}$ in $\mathbf{Z}_q$ from the previous question. Thus there are four distinct solutions $(1, q - 1), (1, 1), (p - 1, 1), (p - 1, q - 1)$. Note that the second and the last are the "standard solutions" 1 and -1 in $\mathbf{Z}_{pq}$

   For example, if $p = 3$ and $q = 4$, in $\mathbf{Z}_{pq} = \mathbf{Z}_{12} = \mathbf{Z}_3 \times \mathbf{Z}_4$, the four solutions $(1, 3), (1, 1), (2, 1)(2, 3)$ correspond to $7, 1, 5$ and 11 respectively. All these solutions on squaring gives 1 modulo 12.