Mid Semester I **Foundations of Computer Science** **Max:30 Marks**

Answer strictly within the space provided
Proper justification to your answers is **absolutely** necessary.

Solution Key ____

1. Let S be an ideal in a ring R. Let $a, b \in R$. Let $x \in a + S$, $y \in b + S$. Show that $xy \in ab + S$. [3]

   Soln: we have $x = a + s_1$, $y = b + s_2$ for some $s_1, s_2 \in S$ by definition. Hence $xy = ab + s_1 b + s_2 a + s_1 s_2$. Since S is an ideal, $s_1 b \in S$, $s_2 a \in S$ and $s_1 s_2 \in S$ (why?). Thus if we set $s = s_1 b + s_2 a + s_1 s_2$, then $xy = ab + s$ with $s \in S$ (why?), or $xy \in ab + S$.

2. Let f be a homomorphism from a ring R to a ring R'. Let $S = \{x \in R : f(x) = 0\}$. Let $a, b \in R$ such that $b \in a + S$. Show that for any $z \in R$, $f(za) = f(zb)$. [3]

   Soln: Since $b \in a + S$, $b = a + s$ for some $s \in S$. Hence $b - a = s \in S$. Therefore, $f(b - a) = f(s) = 0$. Now, $f(zb) - f(za) = f(za - zb) = f(z(a - b)) = f(z)f(s) = f(z).0 = 0$.

3. From the additive group $(\mathbf{R^2}, +)$ to $(\mathbf{R^2}, +)$ define the homomorphism: [3+3]

$$f[x, y] = [x, y] \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}$$

   Find the equations for the set of points in $\mathbf{R^2}$ corresponding to a) $ker(f)$, b) $img(f)$.

   Soln: Clearly, $ker(f) = \{[x, y] : x + y = 0\}$. We claim that $img(f) = \{[x, y] : x + y = 0\}$ as well. For this, take any point $[a, -a]$ for any $a \in \mathbf{R}$. Clearly $f[a, 0] = [a, -a]$. Thus all points in the line $\{[[x, y] : x + y = 0\}$ belongs to $Img(f)$. Moreover, given any $[x, y] \in \mathbf{R^2}$, $f([x, y]) = [x + y, -(x + y)]$ is a point in the line $x + y = 0$. Thus $[x, y] \in Img(f)$ if and only if $x + y = 0$.

4. Let p be an odd prime. If g is a generator of $\mathbf{Z_p^*}$, what is the value of $g^{\frac{p-1}{2}} \mod p$? Justify your answer. [3]

   soln: Let $h = g^{\frac{p-1}{2}} \mod p$. Since $h^2 = g^{p-1} = 1 \mod p$ by Fermat's theorem, h must be a square root of $1 \mod p$. However, $h \neq 1 \mod p$ for in that case, we would have $g^{\frac{p-1}{2}} = 1 \mod p$ which would contradict $o(g) = p - 1$. Hence h must be a square root of 1 other than 1 itself. Since $\mathbf{Z_p}$ is a field, the only square roots of 1 are 1 and $-1 = p - 1 \mod p$. Thus we must have $h = p - 1 \mod p$.

5. How many $a \in \mathbf{Z_p^*}$ will satisfy $a^{\frac{p-1}{2}} = -1 \mod p$? Justify your answer. (Hint: Use the previous question). [3]

   Soln: Let g be a generator of Z_p^*. $(g^i)^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^i = (-1)^i$. Thus if $i = 2k + 1$ for some k, $(g^i)^{\frac{p-1}{2}} = -1$ and if $i = 2k$ for some k, $(g^i)^{\frac{p-1}{2}} = 1 \mod p$. In particular $\{g, g^3, g^5, ..., g^{p-2}\}$ is the set of $\frac{p-1}{2}$ elements which satisfy the property stated in the question.

6. For what values of n between 100 and 110 does 6 generate the additive group $\mathbf{Z_n}$? Justify. [3]

   soln: $(Z_n, +)$ is a cyclic group generated by 1. Thus i generates Z_n if and only if $GCD(i, n) = 1$. When $i = 6$, this is true for for $n \in \{101, 103, 107, 109\}$.

7. Suppose on input $n = 35$, if the random element a in $\mathbf{Z_{15}^*}$ chosen by the Miller Rabin test is 6, what will be the output of the Miller Rabin test? What about the Fermat Test? Give clear justification [3]

   Soln: $6^2 = 1 \mod 35$. Thus $6^k = 6 \mod 35$ when k is odd and $6^k = 1 \mod 35$ when k is even. Both the Fermat's test and the Miller Rabin test finds that $6^{34} = 1$, and this check does not reveal any evidence for compositeness. At this point, Fermat's test returns "prime". Miller Rabin test further evaluates $6^{\frac{35-1}{2}} = 6^{17} = 6 \mod 35$. Since this value is neither 1 nor -1, but is a square root of 1, Miller Rabin test returns "composite". (Note that this question does not assume anything other than a knowledge of the steps performed by the Miller Rabin test and the Fermat's test).

8. Let $p_1, p_2, .., p_n$ be distinct odd primes. Find the smallest positive integer x such that $(p_1 - 1)x = 1 \mod p_1$, $(p_2 - 1)x = 1 \mod p_2$, ..., $(p_n - 1)x = 1 \mod p_n$. You must prove that the x found so is the smallest. Express x as a function of $p_1, ..., p_n$. [3]

   Soln: First observe that $(p_i - 1) = -1 \mod p_i$ for each i. Thus the give system can be reformulated as $-x = 1 \mod p_i$ or equivalently $x = -1 \mod p_i$ for each i. a trivial solution to this set of equations is $x = -1$. To get a positive number, observe that $Z_{p_1 p_2 \ldots p_n}$ is isomorphic to $Z_{p_1} \times Z_{p_2} \times \ldots Z_{p_n}$. Thus $x = -1$ corresponds to $(-1, -1, \ldots -1)$ on the RHS and this corresponds to $x = \prod_{i=1}^{i=n} p_i - 1$ in $Z_{p_1 p_2 \ldots p_n}$. That this value is the least positive such integer follows from Chinese remainder theorem which asserts that there is a unique number x between 0 and $\prod_{i=1}^{i=n} p_i - 1$ satisfying $x = -1 \mod p_i$ for all $1 \leq i \leq n$.

9. Let g be a generator of $\mathbf{Z_p^*}$ that does not generate $\mathbf{Z_{p^2}^*}$. What is the order of g in $\mathbf{Z_{p^2}^*}$? **Prove**. (Use the next page if necessary). [3]

   Soln: Let i be the order of g in $\mathbf{Z_{p^2}^*}$. Since g does not generate $\mathbf{Z_{p^2}^*}$, its order in this group must be a strict divisor of $p(p-1)$. First we show that p does not divide i. Suppose $i = tp$, then $g^{tp} = 1 \mod p^2 \Rightarrow g^{tp} = 1 \mod p \Rightarrow (g^p)^t = g^t = 1 \mod p \Rightarrow (p-1)|t$. However, then $p(p-1)|rt$, or $p(p-1)|i$ which contradicts the fact that g is not a generator of $\mathbf{Z_{p^2}^*}$. Thus we conclude that i divides $p - 1$. We have to prove that $i = p - 1$ to complete the proof.

   Now since i is the order of g in $\mathbf{Z_{p^2}^*}$, $g^i = 1 \mod p^2 \Rightarrow g^i = 1 \mod p$. Since g is a generator of $\mathbf{Z_p^*}$, $g^i = 1 \mod p \Rightarrow (p-1)$ divides i. But i divides $p-1$ and $p-1$ divides i implies that $i = p - 1$.