CS 6101 MFCS IV, Sep.'17. Name:

1. Let $\mathbf{Q}$ and $\mathbf{Z}$ be the set of rational numbers and integers respectively. $\boxed{3+3}$

   1. Is $\mathbf{Z}$ an ideal in the ring $\mathbf{Q}$? Justify your answer.
      Soln: No (easy!). For instance, $3 \in \mathbf{Z}$, $\frac{1}{2} \in \mathbf{Q}$, but $3 \times \frac{1}{2} \notin \mathbf{Z}$.

   2. Consider the Quotient group (with respect to addition) $\frac{\mathbf{Q}}{\mathbf{Z}}$. Give three distinct elements that belong to the same coset as $\frac{3}{5}$. *Soln:* (Easy!). For any $n \in \mathbf{Z}$, $\frac{3}{5} + n$ belongs to the same coset as $\frac{3}{5}$.

2. For what integer values $1 < d < 24$ is it true that $\mathbf{Z}_d$ is a sub-ring of $\mathbf{Z}_{24}$? $\boxed{3}$
   Soln: (Easy!, Conceptual question) For no value of d this can be true. After all, $\mathbf{Z}_d$ is a different ring from $\mathbf{Z}_{24}$ unless $d = 24$ (the addition is different).

3. Specify an ideal I in $\mathbf{Z}_{24}$ with respect which $\frac{\mathbf{Z}_{24}}{I}$ is isomorphic to $\mathbf{Z}_{12}$. Justify your answer. $\boxed{3}$
   Soln: (Intermediate) The map $f : \mathbf{Z}_{24} \mapsto \mathbf{Z}_{12}$ defined by $f(x) = x \mod 12$ is an onto homomorphism with kernel $I = \{0, 12\}$ and image $\mathbf{Z}_{12}$. By homomorphism theorem, $\frac{\mathbf{Z}_{24}}{I}$ is isomorphic to $\mathbf{Z}_{12}$.

4. Let I be an ideal in a ring R. Let $a, b \in R$. Prove that if $x \in a + I$ and $y \in b + I$, $xy \in ab + I$. $\boxed{3}$
   Soln: (Straight forward) Let $x \in a + I$ and $y \in b + I$. Then, by definition, there exists $i, j \in I$ such that $x = a + i$ and $y = b + j$. Hence $xy = ab + (aj + bi + ij) \in ab + I$ because $aj + bi + ij \in I$ (why?).

5. Let $n > 3$ be odd positive integer. Suppose $a \notin \mathbf{Z}_n^*$. Is it always true that $a^{n-1} \neq 1 \mod n$? Justify your answer. $\boxed{3}$
   Soln: (Intermediate) Since GCD$(a, b) \neq 1$, GCD$(a^{n-1}, n) \neq 1$. If $a^{n-1} \equiv 1 \mod n$, then there must be some integer k so that $a^{n-1} - kn = 1$. But this is not possible as GCD$(a^{n-1}, n) \neq 1$ (why?).

6. Suppose p, q are odd primes such that $n = pq$. Suppose both $(p-1)$ and $(q-1)$ divide $n-1$, then prove that n is a Carmichael number. $\boxed{3}$
   Soln: (Non-trivial) Let $a \in \mathbf{Z}_n^*$. By Chinese Reminder Theorem, there exists (unique) $(x, y) \in \mathbf{Z}_p^* \times \mathbf{Z}_q^*$ and $a \equiv x \mod p$ and $a \equiv y \mod q$. By Fermat's theorem $(x, y)^{n-1} = (x^{n-1}, y^{n-1}) = (1, 1)$ in $\mathbf{Z}_p^* \times \mathbf{Z}_q^*$ (why - because $p-1$ and $q-1$ are divisors of $n-1$).

7. For what values of $a \in \{1, 2, \cdots 14\}$ does the equation $ax = 10 \mod 15$ have a solution? $\boxed{3}$
   Soln: (Simple) GCD$(a, 15)$ must divide 10, that is $a \in \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14\}$

8. Let n be odd composite. Suppose there exists $a \in \mathbf{Z}_n^*$ such that $a^{n-1} \neq 1 \mod n$, then show that at least 50% the elements in $\mathbf{Z}_n^*$ does not satisfy $a^{n-1} \neq 1 \mod n$. $\boxed{3}$
   Soln: (Straight forward) The set $S = \{a \in \mathbf{Z}_n^* : a^{n-1} = 1 \mod n\}$ is a subgroup of $\mathbf{Z}_n^*$. Hence, if there exists at least one element in $\mathbf{Z}_n^*$ outside S, then by Lagrange's theorem, S can contain at most half the elements in $\mathbf{Z}_n^*$.

9. Let p, q be odd primes and c, d positive integers such that a) $n = pq$. b) $cd - 1$ is divisible by $(p-1)(q-1)$, can we conclude that every $a \in \mathbf{Z_n}^*$ is a root of the polynomial $x^{cd} - x = 0 \mod n$? $\boxed{3}$
   Soln: (Non-trivial) Note first that $\phi(n) = (p-1)(q-1)$. Hence $cd \equiv 1 \mod \phi(n)$. Now for any $a \in \mathbf{Z}_n^*$, $a^{cd} \equiv a^{1+k\phi(n)} \equiv a.a^{k\phi(n)} \equiv a \mod n$ by Euler's theorem, or $a^{cd} - a \equiv 0 \mod n$.