Quiz

(*reference answers*)

Prof. Manisha Kulkarni, Prof. G.Srinivasaraghavan

On: April 22, 2022	**Time**: 1 Hr	**Max Marks**: 20

1 Part 1

Max Marks: 10

*For **Questions 1 to 4**, state if each of the statements is True or False and justify your answer. In **Question 5** state which options are True and why.*

Q-1: If $r_1, r_2, \cdots, r_p$ and $s_1, s_2, \cdots, s_p$ are two complete residue system mod p where p is a prime greater than 2 and $r_i \neq s_i$ then $r_1s_1, r_2s_2, \cdots, \cdots r_ps_p$ is not a complete residue system.

Answer: **True**

Since $\forall i = 1, \ldots, p, \quad r_i \neq s_i$ and both $r_1, r_2, \cdots, r_p$ and $s_1, s_2, \cdots, s_p$ are complete residue systems it must be that $\exists i \neq j : r_i = s_j = 0 \mod p$. Therefore $r_is_i = r_js_j = 0 \mod p$ implying that the elements $\{r_1s_1, \ldots, r_ps_p\}$ are not all distinct $\mod p$. Therefore $\{r_1s_1, \ldots, r_ps_p\}$ cannot be a complete residue system. ■

Q-2: If a group $G = \{g_1, g_2, \cdots, g_n\}$ is an abelian group of even order having n elements then $(g_1 * g_2 * \cdots * g_n)^2 = e$ where e is the identity element of G.

Answer: **True**

Since G is abelian, the terms in the expression $(g_1 * g_2 * \cdots * g_n) * (g_1 * g_2 * \cdots * g_n)$ can be arranged in any order. Also any g_i has a unique inverse g_i^{-1} and also if $g_i^{-1} = g_j^{-1} \Rightarrow g_i = g_j$. Therefore $(g_1 * g_2 * \cdots * g_n) * (g_1 * g_2 * \cdots * g_n)$ can be rearranged as $(g_1 * g_1^{-1}) * \cdots * (g_n * g_n^{-1}) = e$. ■

Q-3: Every group of prime order is cyclic.

Answer: **True**

Consider any element $g \neq e$ of a group G of prime order p and identity element e. There always exists a $p \geq k > 1$ such that $g^k = e$, where e is the identity element of G — this follows trivially from the finiteness of G. Also $\{e, g, g^2, \cdots, g^{k-1}\}$ is a subgroup of G. Therefore Lagrange's Theorem implies that $k|p$ (the order of the subgoup must divide the order of G). Therefore $k = p$ implying that G is a cyclic group. ■

Q-4: Let G be a group of 36 elements. Let H and K be two subgroups of G of order 4 and 9 respectively then $G = HK = \{h * k : h \in H, \ k \in K\}$.

Answer: **True**

First observation is that $H \cap K = \{e\}$. If $H \cap K$ was non-trivial (other than just $\{e\}$) then it must be closed under the group operation — any $x * y$ with $x, y \in H \cap K$ must obviously belong to both H and K since both H and K are subgroups. So $H \cap K$ is a subgroup of both H and K implying that $|H \cap K|$ divides both $|H|$ and $|K|$ (by Lagrange's Theorem). But that cannot happen in this case since 4 and 9 are co-prime.

If for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$ it is true that $h_1k_1 = h_2k_2$ then $h_2^{-1}h_1 = k_2k_1^{-1}$ implying from the above observation that $h_2^{-1}h_1 = k_2k_1^{-1} = e$. This clearly means $h_1 = h_2$ and $k_1 = k_2$. Therefore nothing repeats in the product HK. Hence the order of HK is $9 * 4 = 36$. Clearly then $HK = G$. ■

Q-5: Let p be a prime number and $U_p = \{n : 1 \leq n \leq p-1\}$. Which of the following are true and why?

(a) U_p is a group under multiplication modulo p.

(b) U_p is isomorphic to the group Z_{p-1} under addition modulo p.

(c) U_p is not abelian.

(d) U_p is not cyclic.

Answer:

(a) **True**: U_p is closed under multiplication because for any $n_1, n_2 \in U_p$, $n_1.n_2 = 0 \mod p \Rightarrow p|n_1$ or $p|n_2$. This is impossible since $n_1.n_2 < p$. Therefore $1 \leq n_1.n_2 \leq (p-1)$. Identity element 1 and associativity are obvious consequences of integer multiplication. Finally there exists a multiplicative inverse $\mod p$ for any $n \in U_p$ since p is prime.

(b) **True**: Since U_p is cyclic, it is true that $U_p = \{a^i \mid i = 1, \cdots, (p-1), a \in U_p\}$ for some element a in U_p. Define a map $\mu : U_p \to Z_{(p-1)}$ where $\mu(a^i) = i$. It is easy to verify that μ is an isomorphism. The thing to note is that multiplication between powers of an element $a \in U_p$ becomes addition between the exponents giving the required homomorphism between the multiplicative group U_p and the additive group $Z_{(p-1)}$. Also $|U_p| = |Z_{(p-1)}| = (p-1)$.

(c) **False**: Modular addition / multiplication over integers is commutative.

(d) **False**: Proof of the fact that U_p is cyclic is quite non-trivial. The expectation is that you should have been able to guess that it is indeed cyclic. Here's a proof that U_p is cyclic for completeness.

Let $p_1^{q_1} * \ldots * p_k^{q_k}$ be the prime factorization of $(p-1)$. Consider the set of elements of $S_i \subset U_p$ defined as $S_i = \{a \mid a^{(p-1)/p_i^{q_i}} = 1 \mod p\}$ for some $i = 1, \ldots, k$. We first observe that $|S_i| < (p-1)$. We know that the count of the number of distinct roots of a real polynomial being at most the degree of the polynomial. An analogue of this also holds for modular equations. So the size of S_i is also bounded by $(p-1)/p_i^{q_i} < (p-1)$. Therefore there exists an element $a_i \in U_p$ for which $a_i^{(p-1)/p_i^{q_i}} \neq 1 \mod p$. Let $b_i = a_i^{(p-1)/p_i^{q_i}}$. Now $b_i^{p_i^{q_i}} = a^{(p-1)} = 1$ from Fermat's Little Theorem. So the order of b_i in U_p divides $p_i^{q_i}$. Suppose the order t_i of b_i in U_p is not $p_i^{q_i}$. Then since p_i is prime, clearly $t_i|p_i^{q_i-1}$. Then since $b_i^{t_i} = 1 \mod p$, it must be that $b_i^{p_i^{q_i-1}} = 1 \mod p$. But $b_i^{p_i^{q_i-1}} = a_i^{(p-1)/q}$ and our choice of a_i was such that $a_i^{(p-1)/q} \neq 1 \mod p$. This is clearly a contradiction. Therefore it must be that the order t_i of b_i is in fact exactly $p_i^{q_i}$.

Finally since $p_i^{q_i}$ for $i = 1, \ldots, k$ are pairwise co-prime, the order of $b_1 * \ldots * b_k$ must be $\prod_{i=1}^{k} p_i^{q_i} = (p-1)$. Therefore $\prod_{i=1}^{k} b_i$ is in fact a generator for U_p. That shows that U_p is cyclic.

■

2 Part 2

Answer the following questions with a short (2-3 lines) justification for each.

Q-1: The sum $\sum_{p\leq x}\frac{1}{\log p} = \theta(\_\_\_\_\_\_\_\_\_\_\_\_)$. **Max Marks: 3**

Answer: $\sum_{p\leq x}\frac{1}{\log p} = \theta\left(\frac{x}{(\log x)^2}\right)$

$$\sum_{p\leq x}\frac{1}{\log p} \geq \sum_{\sqrt{x}\leq p\leq x}\frac{1}{\log p} \geq \frac{1}{\log x}\left(\pi(x)-\pi(\sqrt{x})\right) = \frac{\pi(x)}{\log x}\left(1-\frac{\pi(\sqrt{x})}{\pi(x)}\right) \approx \frac{x}{(\log x)^2}$$

To show the upper bound let's first assume that x is a positive integer and carry out an induction on x. Assume for all $n < x$, $\sum_{p\leq n}\frac{1}{\log p} \leq O\left(n/(\log n)^2\right)$. Then

$$\begin{aligned}
\sum_{p\leq x}\frac{1}{\log p} &= \sum_{p\leq\sqrt{x}}\frac{1}{\log p} + \sum_{\sqrt{x}<p\leq x}\frac{1}{\log p}\\
&\leq \frac{\sqrt{x}}{(\log\sqrt{x})^2} + \frac{1}{\log\sqrt{x}}\left(\pi(x)-\pi(\sqrt{x})\right)\\
&= \frac{4\sqrt{x}}{(\log x)^2} + \frac{2\pi(x)}{\log x}\left(1-\frac{\pi(\sqrt{x})}{\pi(x)}\right)\\
&= \frac{4\sqrt{x}}{(\log x)^2} + \frac{2x}{(\log x)^2}\left(1-\frac{\pi(\sqrt{x})}{\pi(x)}\right)\\
&\leq \frac{cx}{(\log x)^2} \quad \text{for some constant } c
\end{aligned}$$

In step 2 of the above upper bound calculation, we have invoked the induction hypothesis for the first term and the second term is a simple upper bound based on the max term in the series and the number of terms in the series.

Finally for any real x we have

$$\sum_{p\leq x}\frac{1}{\log p} = \sum_{p\leq\lfloor x\rfloor}\frac{1}{\log p} \leq \frac{c\lfloor x\rfloor}{(\log\lfloor x\rfloor)^2} \leq \frac{cx}{(\log(x-1))^2} \leq \frac{cx}{(\log\sqrt{x})^2} = \frac{4cx}{(\log x)^2}$$

Note: This answer is in its full rigor. I was expecting just the first line (or something similar) for the upper and lower bound in your answers. ■

Q-2: Use rational reconstruction to find a rational approximation for $\pi \approx 3.141592654$ correct up to 6 decimal digits, where the denominator of the approximating rational is at most 1000.
Max Marks: 4
Answer: Let $M = 1000$ (upper bound on the denominator). $n = 10^6$ and $b = 141592$. Let $r^* = t^* = M$. Running EGCD on the pair (n, b) we get
So $\pi \approx 3 + \frac{16}{113} = \frac{355}{113}$. ■

Q-3: Match the quantities on the left column with the order of magnitude of these quantities on the right. In all the options below p refers to a prime number, x is some positive real number, n is some positive integer and $\omega(n)$ is the number of prime divisors of a positive integer n.
Max Marks: 3

r	q	s	t
1000000		1	0
141592	7	0	1
8856	15	1	-7
8752	1	-15	106
104	84	16	-113

a $\sum_{p\le x} \log p$

b $\sum_{p\le x} 1/p$

c $\prod_{p\le x}(1-1/p)$

d $\omega(n)$

e $\sum_{p\le x}(\log p)/p$

f $\prod_{2<p\le x}(1-2/p)$

1. $\theta(\log x)$
2. $\theta(x)$
3. $\theta\left(1/(\log x)^2\right)$
4. $O\left(\log n/\log\log n\right)$
5. $\theta(\log\log x)$
6. $\theta(1/\log x)$

Answer: A few observations will make the matching obvious:

- Clearly $\sum_{p\le x}\log p > \sum_{p\le x}(\log p)/p > \sum_{p\le x} 1/p$. In any case all these sums were derived in the class.
- $\left(\prod_{p\le x}(1-1/p)\right)^2 = \prod_{p\le x}(1-1/p)^2 \approx \prod_{p\le x}(1-2/p)$. The last approximation follows from a simple binomial expansion of $(1-1/p)$ and ignoring the quadratic term $1/p^2$.
- $\omega(n)$ is the odd-one out defined on an *integer* n!!

From the above it should be easy to infer that:

$$\sum_{p\le x}\log p = \theta(x)$$

$$\sum_{p\le x}(\log p)/p = \theta(\log x)$$

$$\sum_{p\le x} 1/p = \theta(\log\log x)$$

$$\prod_{p\le x}(1-1/p) = \theta(1/\log x)$$

$$\prod_{2<p\le x}(1-2/p) = \theta\left(1/(\log x)^2\right)$$

$$\omega(n) = O\left(\log n/\log\log n\right)$$

As a corollary we should be able to see also that $\prod_{2<p\le x}(1-k/p) = \theta\left(1/(\log x)^k\right)$ for $k \ge 1$.■