CS 201 End Semester Exam

Mahaarajan J-220600

21st November 2023

1a.

First we shall use

Fermat's Little Theorem
Proof: For any prime number p, and any integer a, the following equation holds:
$a^p \equiv a \pmod{p}$ now when, a is not a multiple of p we can multiply a on both sides to get
$a^{p-1} \equiv 1 \pmod{p}$.
We shall now prove this using Induction
The base case, $1^p \equiv p \pmod{p}$, is obviously true. Suppose the congruence, $a^p \equiv a \pmod{p}$ also holds.
Then, by the binomial theorem, we have, $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + ... + \binom{p}{p-1}a + 1$ Also, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ Since, p is prime, p divides the numerator and not the denominators (as both the factorial terms in the denominator are less than p hence p factor can't appear in the denominator), hence the term $\binom{p}{k}$, is divisible by p, for $1 \leq k \leq p-1$.
Hence on applying mod(n) all the middle terms disappear and only the first and last terms are left. Thus, we get
$(a+1)^p \equiv a^p + 1 (\bmod p)$ Using, the known congruence, $a^p \equiv a \pmod{p}$, we get,$(a+1)^p \equiv a + 1 (\bmod p)$
Hence Proved

Given a bipartite graph $G = (U, V, E)$, a Prefect Matching of G is a map $\sigma : U \longrightarrow V$ such that :

- $\sigma(u)$ is one-to-one and onto function.
- For all, $u \in U$, the edge, $(u, \sigma(u)) \in E$

a) **To Prove:**The Graph G has a perfect matching, if $F = F_{71}$ We shall try to prove that the mapping of (a, a^3) over the field, F_{71} satisfies both the properties that $\sigma(a)$ satisfies for a perfect mapping.
We first prove that for every a, the operation a^3, over this field, is unique for $a \in [0, 70]$.
From multiplying the equations of Fermat's theorm
$a^{2p-1} \equiv a \pmod{p}$ For $p = 71$, for $a \in [0, 70]$,
$a^{141} \equiv a \pmod{71}$
$(a^3)^{47} \equiv a \pmod{71}$
Claim: For $a \in [0, 70]$, $(a^3) \equiv l \pmod{71}$ l, will be unique for every a.
We shall try to prove this claim by contradiction.
Assume, that l, is not unique for some $a, b \in [0, 70]$ then for and $a \neq b$ we will have $(a^3) \equiv l \pmod{71}$, $(b^3) \equiv l \pmod{71}$ Now, raising both of these concurrences to the 47^{th} power, we get, $(a^3)^{47} \equiv l^{47} \pmod{71}$
$(b^3)^{47} \equiv l^{47} \pmod{71}$
Now a^{141} and a have the same remainder and same is true for b. Hence we are getting that a and b have the same remainder when divided by 71.
Hence we have arrived at a contradiction.
Therefore, we have proved that, modulus of a^3, taken with 71, will map every number $a \in [0, 70]$ to a unique number $l \in [0, 70]$.
Hence the number of neighbours of a subset will always be greater than or equal to the size of that subset for any subset as there will always be more than or equal to n outgoing edges.
Also we are going to choose $\sigma(a)$ as a^3 as a^3 is unique for all values of a making it one-one and onto, also by definition (a, a^3) is an edge.
Also we do not require to consider the edges (a, a^2) as we have proved the neighbourhood theorem by considering (a, a^3).

Hence Proved

1b.

To Show: The Graph G does not have a perfect matching, if the field F is F_{73} For $W \subseteq U$, we define $N(W) = \{U \in V | (u, v) \in E$ for some $u \in W\}$.

As seen in the lectures and previous part, if in a bipartite graph, for some $W \subseteq U$, $|N(W)| < |W|$ then, there will be no perfect matching for this graph G.

Consider the following counter-example:

Consider the subset $W = \{1, 9, 64, 72\}$. For this W we will have the following edges (a, a^3) as {(1,1),(9,72),(64,1),(72,72)} and the edges (a, a^2) will be {(1,1),(9,8),(64,8),(72,1)}, $N(W) = \{1, 8, 72\}$ (by considering both (a, a^2) and (a, a^3) edges). There is one more subset as well $W = \{1, 8, 65, 72\}$ in which the edges (a, a^3) will be {(1,1),(8,1),(65,72),(72,72)} (a, a^2) will be {(1,1),(8,64),(65,64),(72,1)}for which $N(W) = \{1, 8, 72\}$

Since, size of neighbourhood is 3 which is less than the size of the subset (4) hence, the above statement is satisfied and hence the graph G does not have a perfect matching if $F = F_{73}$

Hence Dis-Proved

2a.

To Prove: ϕ related is an equivalence relation.

Reflexive: **Claim:** Any permutation can be expressed as a combination of disjoint cycles (sequence of numbers such that if the permutation is applied repeatedly we get back the starting number)
Proof: Consider a permutation σ on X. Let an arbitrary $x_1 \in X$, and consider the changes to x_1 under σ: $\text{Path}_\sigma(x_1) = \{x_1, \sigma(x_1), \sigma^2(x_1), \ldots\}$
Since size(X) is finite, by Pigeonhole principle ,there must be a smallest positive integer k such that $\sigma^k(x_1) = x_1$ (otherwise, the path would be infinite). This would give us the cycle $C_1 = (x_1, \sigma(x_1), \sigma^2(x_1) \ldots \sigma^{k-1}(x_1))$.
Now, remove the elements involved in the cycle, and if there are remaining unexplored elements, repeat the process until all elements are part of cycles and no element is un-visited.
This process will end as at least one element is removed from consideration in each step,and since X is finite, the process must eventually terminate.
Therefore, This process would break down σ into disjoint cycles.
Hence Proved
Now let the permutation ϕ be broken down into k cycles $C_1, C_2, ..., C_k$ with lengths $L_1, L_2, ..., L_k$. Now if we apply ϕ for $m * L_i$ (where m is a natural number) times then all the elements of C_i will retain their positions (as if we go around the loop m times completely).
Hence if we apply ϕ j times such that j=LCM($L_1, L_2, ...L_k$) then all the elements would retain their positions (as each element is part of one of these cycles).
Hence there exists o such that $\phi^o C = C$.
Hence Proved it is reflexive.

Symmetric: Let $C_1 R C_2$ then we will have $\phi^j C_1 = C_2$ for some $j > 0$. Since ϕ is a bijection there will be an inverse ϕ^{-1}.
Let us apply ϕ^{-j} (applying ϕ^{-1} both sides j times) to get $C_1 = \phi^{-j} C_2$.
Now from the first part there will be o such that $\phi^o = I$, there will exist a p such that $p * o > j$, applying ϕ^{p*o} on the rhs (as ϕ^o is identity we can apply it p times without any changes).
Hence we will have $C_1 = \phi^{p*o-j} C_2$ and $p * o - j > 0$. Therefore $C_2 R C_1$.
Hence Proved it is symmetric

Transitive: Let $C_1 R C_2$ and $C_2 R C_3$. Hence we can write $\phi^j C_1 = C_2$ and $\phi^l C_2 = C_3$ where $j, k > 0$. Applying ϕ^l on both sides of the first equation we have $\phi^{j+l} C_1 = \phi^l C_2 = C_3$ hence there is j'=j+l such that $\phi^{j'} C_1 = C_3$ hence $C_1 R C_3$. Therefore we have proved it is transitive.

Hence Proved that R is an equivalence relation

2b.

By observation we can see that the given permutation has 3 cycles for lengths 3,5 and 7 respectively. They are (10,12,14,10),(1,3,7,11,4,1) and (2,8,5,13,6,15,9,2).

Now we can observe that the lengths of the cycles are co-prime and the cycles are independent i.e one element is part of only one cycle. We can divide each coloring into coloring of its cycles C_3, C_5, C_7. Now if we apply ϕ once then we will shift each colour in the cycles by one place.

Let us find the number of permutations of arranging 3 colours in a circular manner in cycles of the required lengths, let the number of such permutations be P_3, P_5, P_7 respectively for the given cycles.
This is because if we apply ϕ on any of C_1,C_2 or C_3 it is just like rotating a cycle, hence we calculate the number of circular permutations.

Hence it will be same as the number of arrangements on 3 circular tables of sizes 3,5,7 with three colours {A,B,C} and can be seen as a counting necklaces problem with different symmetries.
The symmetries here are S_3 (rotation of a 3 sided table) S_5 (rotation of a 5 sided table) and S_7 (rotation of a 7 sided table)
Hence the group of symmetries is

$$S = \{{S_3}^i, {S_5}^j, {S_7}^k | 0 \leq i < 2, 0 \leq j < 4, 0 \leq k < 6\}$$

Let $\sigma \in S$ (a symmetry) define N_S

$$N_S = \{\sigma | \sigma(s) = s, \sigma \in S\}$$

(the number of arrangements that remain unchanged when the symmetry is applied) From the notes to calculate the number of permutations we use the function

$$\sum_S \frac{|N_S|}{|S|}$$

Number of symmetries=3.5.7=105 (as there are 3 choices for i,5 for j and 7 for k)
Hence we can write the equation as

$$\frac{1}{105} \sum_S |N_S|$$

Assuming same definition of F_σ as in notes, the set of sequences $\{s|\sigma(s) = s, s \in S\}$ (the sequences that are unchanged on application of the permutation σ

$$= \frac{1}{105}\sum_{\sigma \in S}|F_\sigma|$$

Now consider the following similar to as done in class notes first consider only the symmetries of the 3 sized ring as it is isolated hence the rest will just be multiplications of the rest. As the rings are independent of each other

$|F_0| = 3^3$ (equivalent to the case where no permutation is applied, hence all sequences are unchanged)

$$|F_{S_3}| = 3$$

(in this case only the sequences with all their elements equal are preserved)

$$|F_{S_3{}^2}| = 3$$

In general for a ring of size n for 3 colors and the i^{th} rotational symmetry (ψ^i) (as used in class)

$$|F_{\psi^i}| = 3^{gcd(i,n)}$$

So we get in general for non zero values of i,j,k we can write

$$|F_{S_3{}^i S_5{}^j S_7{}^k}| = 3^{gcd(i,3)} \cdot 3^{gcd(j,5)} \cdot 3^{gcd(k,7)}$$

if any of i, j, k is zero just replace that term with 3^n where n is the ring size.

Hence number of permutations are,

$$\frac{1}{105}\sum_{\sigma \in S}|F_\sigma|$$

because 3,5,7 are prime the gcd in each case will be 1. Now we will take different cases:

- None are 0, value is $2 * 4 * 6 * 3^3 = 1296$
- One is zero,
  - $i = 0$, $3^3 * 4 * 6 * 3^2 = 5832$
  - $j = 0$, $3^5 * 2 * 6 * 3^2 = 26244$
  - $k = 0$, $3^7 * 2 * 4 * 3^2 = 157464$
- Two are zero,
  - $i, j = 0$, $3^8 * 6 * 3 = 118098$
  - $j, k = 0$, $3^{12} * 2 * 3 = 3188646$
  - $k, i = 0$, $3^{10} * 4 * 3 = 708588$
- All three are 0, $3^{15} = 14348907$

Adding all the elements we have it equal to 18555075
Hence the final answer will be $\frac{18555075}{105} = \mathbf{176715}$
The final answer will be **176715**

Hence Proved

2c.

The permutation providing the maximum number of unrelated colorings (equivalence classes) would be the identity permutation I where all positions are mapped to themselves.
This would imply that for $C_1 R C_2$ we have $\phi^j C_1 = C_2$ which simplifies to $C_1 = C_2$ as ϕ is identity.
Hence all distinct C's will be unrelated colouring. This will be the maximum number of unrealted colorings as each possible colouring is unrelated.
Let us take any ϕ which is not identity then there will exist a C_i such that $\phi C_i = C_j$ such that $C_i \neq C_j$ (if there is no such C_i it would imply that ϕ is an identity)

Hence $C_i R C_j$ therefore the number of unrelated colourings will be less than the total number of possible colourings.
Hence the identity permutation does indeed produce the maximum number of un-related colourings.

Hence Proved

3a.

Example: Let us consider the F to be the field of real numbers and the transcendental number α to be e (euler's constant).

Claim: e is a transcendental number.

Proof: Observe that, if $f(x)$ is any real polynomial with degree m, and if,

$$I(t) = \int_0^t e^{t-u} f(u) du,$$

where, t is an arbitrary complex number and the integral is taken over the line joining O and t, then, by repeated integration by parts, we have,

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t). \tag{1}$$

Further, if $\bar{f}(x)$ denotes the polynomial obtained from f by replacing each coefficient with its absolute value, then

$$|I(t)| \leq \int_0^t |e^{t-u} f(u)| du \leq |t| e^{|t|} \bar{f}(|t|). \tag{2}$$

Suppose now that e is algebraic, so that,

$$q_0 + q_1 e + ... q_n e^n = 0 \tag{3}$$

for some integers $n > 0$, $q_0 \neq 0, q_1, ..., q_n$. We shall compare estimates for,

$$J = q_0 I(0) + q_1 I(1) + ... q_n I(n),$$

where $I(t)$ is defined as above with,

$$f(x) = x^{p-1}(x-1)^p ... (x-n)^p$$

p denoting a large prime. From (1) and (3) we have,

$$J = -\sum_{j=0}^{m} \sum_{k=0}^{m} q_k f^{(j)}(k),$$

where $m = (n+1)p - 1$. Now clearly $f^{(j)}(k) = 0$ if, $j < p, k > 0$ and if $j < p-1, k = 0$, and thus for all j, k other than $j = p-1, k = 0$, $f^{(j)}(k)$ is an integer divisible by $p!$; further we have

$$f^{(p-1)}(0) = (p-1)!(-1)^{np}(n!)^p,$$

whence, if $p > n$, $f^{(p-1)}(0)$ is an integer divisible by $(p-1)!$ but not by $p!$. It follows that, if also $p > |q_0|$, then J is a non-zero integer divisible by $(p-1)!$ and thus $|J| \geq (p-1)!$. But the trivial estimate $\bar{f}(k) \leq (2n)^m$ together with (2) gives,

$$|J| \leq |q_1|e\bar{f}(1) + ... + |q_n|ne^n\bar{f}(n) \leq c^p$$

for some c independent of p. The estimates are inconsistent if p is sufficiently large and the contradiction proves the theorem.

Hence Proved

3b.

To Prove: F[α] is a field. Let us consider a function g from F[x] to F[α] given by G(f(x))=f(α), then G is a ring homo-morphism as:

- We know $G(f_1(x) + f_2(x)) = f_1(\alpha) + f_2(\alpha) = (f_1(\alpha)) + (f_2(\alpha)) = G(f_1(x)) + G(f_2(x))$
- Similarly $G(f_1(x) * f_2(x)) = f_1(\alpha) * f_2(\alpha) = (f_1(\alpha)) * (f_2(\alpha)) = G(f_1(x)) * G(f_2(x))$

Hence G is indeed a ring homo-morphism Let us now try to prove some claims.

Claim 1: p(x) is irreducible over F
Proof p(x) is the minimal polynomial of α over F_0 of degree d. We can assume coefficient of x^d to be 1 as F_0 is a field. By contradiction if there exist polynomials g,h such that p=gh (assume p is reducible) and g,h will be in F[x] such that deg(g(x)),deg(h(x)) $< d$. Now as F is a feild since coeffecients of h(x) and g(x) are in F[x] and $\alpha \in F$ we can say that f(α) and g(α) will be in F.
Then from definition of α we will have $p(\alpha) = g(\alpha)h(\alpha) = 0$ which implies either f or g is 0 at α (as additive identity is unique in F). Hence we have got polynomials in F_0 with degree $< d$ and root as α.
This is a contradiction to minimality of degree of p.
Hence p is irreducible over F_0.
Hence Proved

Claim 2: If p(x) is irreducible then it is the maximal ideal
Proof: If $< p(x) >$ is not the maximal ideal then let there be a maximal ideal I of F[x] such that I=$< g(x) >$.
Hence we must have p(x)=g(x)h(x), but we know p is irreducible hence I can't exist hence p is the maximal ideal.
Claim 3: G(F[x]) is isomorphic to F[x]/$< p(x) >$
Proof:
Since the degree of $p(\alpha)$ is d, we can write each element of $F[x]/ < p(x) >$ uniquely in the form :

$a_{d-1}x^{d-1}+\cdots+a_0+<p(x)>= [a_{d-1}x^{d-1}+\cdots+a_0], (a_0, \cdots, a_{d-1} \in F)$

as is obvious from the definition of quotienting and has been shown in class.
Also

$G(a_{d-1}x^{d-1}+\cdots+a_0+<p(x)>) = G(a_{d-1}x^{d-1}+\cdots+a_0)+G(<p(x)>)$

Also we know $G(<p(x)>) = 0 \because <p(x)>$ is the kernel so we get,

$$G(a_{d-1}x^{d-1} + \cdots + a_0 + <p(x)>) = G(a_{d-1}x^{d-1} + \cdots + a_0)$$

(the second term becomes 0) So for each element $t \in [a_{d-1}x^{d-1}+\cdots+a_0]$, we get $G(t) = G(a_{d-1}x^{d-1} + \cdots + a_0)$
Now let us consider any two polynomials belonging to different equivalence class $t_1 \in [P_1], t_2 \in [P_2]$, Here P_1, P_2 are polynomials with co-efficients form F and *degree* $\leq d$. $G(t_1 + t_2) = G(t_1) + G(t_2) = G(P_1) + G(P_2)$ Also consider, $G(t_1 * t_2) = G(t_1) * G(t_2) = G(P_1) * G(P_2)$

Consider a map $\psi : G(F[x]) \to F[x]/ <p(x)>$.

$$\psi(G(a_{d-1}x^{d-1} + \cdots + a_0)) = [a_{d-1}x^{d-1} + \cdots + a_0]$$

Consider the following relation,

$$\psi(G(f_1(x) + f_2(x))) = [f_1(x)] + [f_2(x)] = \psi(G(f_1(x))) + \psi(G(f_2(x)))$$

Similarly doing it for the other group operation *,

$$\psi(G(f_1(x) * f_2(x))) = [f_1(x)] * [f_2(x)] = \psi(G(f_1(x))) * \psi(G(f_2(x)))$$

Hence ψ is a Homomorphism.

Also for all such different $G(f(x))$ that give the same value we will get the unique $[P(x)]$ hence ψ is one-one.
Moreover for each $[P(x)]$ there is at least one $G(P(x))$ that maps to it, hence ψ is onto.
Hence ψ is an isomorphism and $G(F[x]) \cong F[x]/ <p(x)>$
We have proved the Lemma

By definition we know that $\phi(F[x]) = F[\alpha]$.
$\implies F[\alpha] \cong F[x]/ <p(x)>$, hence $F[\alpha]$ is a field.

3c.

Given information: F_j and F_0=$\mathbb{Q}$.Ring R_j=F_{j-1}[x].

To Prove: $x^2 - 5^{1/2^{j-1}}$ is irreducible over the ring R_j.

Proof: Consider α=$5^{1/2^j}$.
Clearly, $5^{1/2^j}$ does not belong to F_{j-1} (hence there is no polynomial of degree 0)

Now, suppose there is a first-degree monic polynomial f(x) in F_{j-1}[x] such that this is the minimal polynomial of α.
Since f(β)=0, f(x) will be of the form x-$5^{1/2^j}$. However, the constant term in this polynomial, $5^{1/2^j}$ doesn't belong to F_{j-1}. Hence, f(x) can't belong to the ring R_j. Therefore there is no possible f(x) with degree 2.

The next higher degree is 2. Consider the polynomial f(x) = $x^2 - 5^{1/2^j}$.
Clearly, f($5^{1/2^j}$)=$(5^{1/2^j})^2 - 5^{1/2^{j-1}}$ = 0.

Thus, we get the lowest degree polynomial (since we have checked all degrees below it) with coefficients in F_{j-1}(which has already been proven to be a field) such that f(α)=0. This is the minimal polynomial in F_{j-1}.

It has already been proven in 3(b) that a minimal polynomial in field F is going to be irreducible in the ring F[x].

Hence Proved

3d.

$x^2 - 5^{1/2^{j-1}}$ is irreducible it is a maximal ideal as proved above. Now if R_j is a ring, $G = R_j/I$ is a field for I being the maximal ideal (Proved in class)

We also know $G \cong F_{j-1}[\alpha_j] = \mathbb{Q}[\alpha_{j-1}][\alpha_j]$, Now we need to prove an isomorphism between G and F_j, which is equivalent to proving $F_{j-1}[\alpha_j] \cong F_j = \mathbb{Q}[\alpha_j]$ or $F_{j-1}[\alpha_j] \cong \mathbb{Q}[\alpha_j]$.
So we basically have to prove a isomorphism between

$$\{f_0 + f_1\alpha_j + \cdots | f_0, \cdots \in F_{j-1}\}$$

and

$$\{q_0 + q_1\alpha_j + \cdots | q_0, \cdots \in \mathbb{Q}\}$$

. Hence we will try to prove a bijective function R:$F_{j-1} \to \mathbb{Q}$. We can use that to show that R is a bijection and therefore there will be an isomorphism between the 2 fields $f = \{a_0 + a_1\alpha_{j-1} + \cdots | a_0, \cdots \in \mathbb{Q}\}$. Because $\alpha = 5^{1/2^{j-1}}$ after some power of α, t we get $\alpha^t = 5$, after which the irrational part will repeat by PHP as there are only finitely many different irrational parts,hence the entire f can be rewritten as

$$f = \{b_0 + b_1\alpha_{j-1} + \cdots + b_{t-1}\alpha_{j-1}^{t-1} | b_0, b_1, \cdots \in \mathbb{Q}\}$$

Now consider $b_i = \frac{n_i}{d_i}$ where n_i, d_i are integers by definition of rational numbers we can write all the b_i's in this way.
A one-one map from F_{j-1} to $\mathbb{Q}$ would be:

f maps to a rational number defined by

$$p_1^{n_1} p_2^{n_2} \cdots . q_1^{d_1} q_2^{d_2} \cdots$$

, where $p_i's, q_i's$ are distinct prime numbers. Since all are distinct prime numbers we can say that we will get a unique rational number for one series of $\{n_1, n_2, n_3 .... d_1, d_2, d_3 ...\}$
as if it is same for 2 different sequences then they must have the same prime factorisation which will be a contradiction as the sequences are different.
Hence Proved one-one.

We can also define a one-one map from $\mathbb{Q}$ to F_{j-1}, such that for each $q \in \mathbb{Q}$, each $b_i = q$. This will be one one as for a different value of q we will have a different sequence of b_i's.
Hence we have a one-one map in each direction so we can form a bijection between F_{j-1} and $\mathbb{Q}$, say ϕ (defined by the Cantor-Bernstein theorem discussed in class)
So consider the map $\psi : F_{j-1}[\alpha_j] \to \mathbb{Q}[\alpha_j]$, such that,
$\psi(\{f_0 + f_1\alpha_j + \cdots | f_0, \cdots \in F_{j-1}\}) = \{\phi(f_0) + \phi(f_1)\alpha_j + \cdots | \phi(f_0), \cdots \in \mathbb{Q}\}$.
This is clearly an isomorphism because ϕ is a bijection.

Hence Proved $\implies \mathbf{\hat{F} \cong F_j}$

[1]

---

[1]

References:

- AOPS Wiki for proof of Fermat's Little Theorm
- Alan Baker. *Transcendental Number Theory*. Cambridge University Press, First edition, 1975 for proof of e being transcendental
- Joseph A. Gallian. *Contemporary Abstract Algebra*. Cengage, Ninth Edition, 2017.