CS201

End-Semester

Kushagra Srivastava

Question 1

Fermat's Little Theorem

For any prime number p, and any integer a, the following congruence holds:

$$a^p \equiv a \ (\text{mod} p)$$

when, a is not a multiple of p, it is equivalent to,

$$a^{p-1} \equiv 1 \ (\text{mod} p)$$

Proof. We will follow a inductive proof in order to prove this identity.
The base case, $1^p \equiv 1 \ (\text{mod} p)$, is obviously true. Suppose the congruence, $a^p \equiv a \ (\text{mod} p)$ 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 will divide $p!$, but it will not divide wither of $k!$ or $(p-k)!$, as both of, $k!$ or $(p-k)!$, will not contain any multiple of p. Thus, p does not divide the denominator but divides the numerator, hence the factorial, is divisible by p, for $1 \leq k \leq p-1$.
Taking the binomial expression $(\text{mod} p)$, all the middle terms disappear, leaving the end terms.
Thus, we get,

$$(a+1)^p \equiv a^p + 1 (\text{mod} p)$$

Using, the known congruence, $a^p \equiv a \ (\text{mod} p)$, we get,

$$(a+1)^p \equiv a + 1 (\text{mod} p)$$

Perfect Matching

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

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

▷ The Graph G has a perfect matching, if $F = F_{71}$

Our goal is to prove that the such a mapping $\pi(a)$ of (a, a^3) over the field, F_{71} exists. We first prove that for every a, the operation a^3, over this field, is unique for $a \in [0, 70]$. Fermat's Little Theorem along with a trivial observation gives us (1) and (2).

$$a^{p-1} \equiv 1 \ (\text{mod} p) \tag{1}$$

$$a \equiv a \ (\text{mod} p) \tag{2}$$

Squaring (1), and multiplying it with (2), we get,

$$a^{2p-1} \equiv a \ (\mathrm{mod} p) \tag{3}$$

For $p = 71$,

$$a^{141} \equiv a \ (\mathrm{mod} 71)$$

$$(a^3)^{47} \equiv a \ (\mathrm{mod} 71) \tag{4}$$

Assertion: For $a \in [0, 70]$, i.e a $\in F_{71}$,

$$(a^3) \equiv l \ (\mathrm{mod} 71)$$

l, will be unique for every a, and l will belong to this field.

Proof. Assume, that l, is not unique for some $a, b \in [0, 70]$, and $a \neq b$

$$(a^3) \equiv l \ (\mathrm{mod} 71)$$

$$(b^3) \equiv l \ (\mathrm{mod} 71)$$

Now, raising both of these concurrences to the 47^{th} power, we get,

$$(a^3)^{47} \equiv l^{47} \ (\mathrm{mod} 71)$$

$$(b^3)^{47} \equiv l^{47} \ (\mathrm{mod} 71)$$

Here clearly, if $a \neq b$, the above two equations can not yield the same result, hence 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 $l \in [0, 70]$. Thus the map $\pi(u)$ is **one-to-one**.
We also know, that if $f(x)$ is a one-to-one function and the cardinality of both the range and the co-domain are equal, this implies that the function is onto as well, and hence it is bijective.
Since both a and a^3, belong to this field, this implies that $a \in [0, 70]$ and $a^3 \in [0, 70]$. Thus, the cardinality of the domain is 71 and the cardinality of the range (which has to be equal to the co-domain here) is also 71. Thus, the function is **onto**.
Hence, this graph has a perfect mapping over F_{73}

▷ The Graph G does not have a perfect matching, if $F = F_{73}$

For $W \subseteq U$, we define $N(W) = \{U \in V | (u, v) \in E \text{ for some } u \in W\}$.
As seen in the lectures, if in a bipartite graph, for some $W \subseteq U$,

$$|N(W)| < |W|$$

then, there is no perfect matching for this graph G.
Consider the subset $W = \{1, 9, 64, 72\}$. For this W we have, $N(W) = \{1, 8, 72\}$

Since, $|N(W)| = 3$ and $|W| = 4$, the above statement is satisfied and hence the graph G does not have a perfect matching if $F = F_{73}$

Question 2

▷ "ϕ-related" is an equivalence relation

Claim: Every permutation can be broken into a set of disjoint cycles.

Proof. Consider a permutation σ of a finite set $X = [1, n]$. For an arbitrary element $x_i \in X$, consider the set, with operations under σ

$$\text{Path}_{\sigma(x_1)} = \{x_1, \sigma(x_1), \sigma^2(x_1), \ldots\}$$

Given, X is a finite set, using the *Pigeon Hole Principle*, there must exist a smallest k, such that $\sigma^k(x_1) = x_1$. Thus the path is finite. This gives us our first cycle $C_1 = (x_1, \sigma(x_1), \sigma^2(x_1) \ldots \sigma^{k-1}(x_1))$.
Now, discard the vertices that have appeared in this cycle C_1, and repeat this process for the remaining "unvisited" elements, to obtain newer cycles, until all elements are part of a cycle, and no element is unvisited. This process is finite, and will eventually end, as at least one element is removed form the set in each iteration.
Thus, this construction breaks down the permutation into disjoint cycles.

- **Reflexive** Consider the permutation ϕ, which can be broken into k disjoint cycles $C_1, C_2, \ldots C_k$, with lengths $L_1, L_2, \ldots L_k$. If we apply, the operation ϕ, $\text{lcm}(L_1, L_2, \ldots L_k)$ times, all the elements would retain their positions, Hence, there exists a j, such that $\phi^j(C_1) = C_1$.
  Therefore, C_1 is related to itelsef.
- **Symmetric**
  We know that the function ϕ is a bijective function, thus it must have an inverse, ϕ^{-1}.
  Consider C_1, C_2, such that C_1 is related to C_2. Thus for some $j > 0$, $\phi^j(C_1) = C_2$. On applyong the operation ϕ^{-1} j times on this relation, we get $C_1 = \phi^{-j}(C_2)$.
  We also know that, there will be a k such that ϕ^k is an identity function. Clearly, there will exist a p such that $pk > j$. Applying the operation $\phi^{pk} = I$ on the obtained inverse relation, we get,
  $$I(C_1) = \phi^{pk-j}(C_2)$$
  $$\phi^{j'}(C_2) = I(C_2)$$
  with $j' = pk - j > 0$ Hence, C_2 is related to C_1. Thus, it is a symmetric relation.
  $$\phi^{j_1+j_2}(C_1) = \phi^{j_2}(C_2) = C_3$$
  Hence, C_1 is related to C_3. Thus, function is transitive.
- **Transitive**
  Consider C_1, C_2 and C_3, such that C_1 is related to C_2, and C_2 is related to C_3. This implies that we can write, $\phi^{j_1}(C_1) = C_2$ and $\phi^{j_2}(C_2) = C_3$, where $j_i > 0$. On applying the function ϕ^{j_2} on both sides of the relation between C_1 and C_2, we have,
  $$\phi^{j_1+j_2}(C_1) = \phi^{j_2}(C_2) = C_3$$
  Hence, C_1 is related to C_3. Thus, function is transitive.

Since, ϕ is reflexive, symmetric and transitive, the it is an equivalence relation.

▷ Number of unrelated colourings for the given permutation.

Let us first compute the cycles in the given permutation,

- $10 \to 12 \to 14 \to 10$
- $1 \to 3 \to 7 \to 11 \to 4 \to 1$
- $2 \to 8 \to 5 \to 13 \to 6 \to 15 \to 9 \to 2$

The three cycles have lengths, 3, 5 and 7 respectively, and all three of them are co-prime numbers. The cycles are also disjoint, i.e all elements in a particular cycle belong to only one cycle. Let's name these cycles as X_3, X_5, X_7.

Claim: The total number of equivalence classes, will be equal to the number of different permutations that can not be inter-converted to one another by applying the ϕ operation a finite number of times.

Consider a coloring C, which belongs to an equivalence class E. C, will have some coloring of the its cycle, X_3, X_5, X_7, then applying ϕ is basically, shifting each color in its cycle by one place. For eg, in X_5, applying ϕ would imply shifting the color at 1 to 3, the color at 3 to 7 and so on till the color at 4 is shifted to the color at 1.
The number colorings of circular permutation P_i, for X_i will be equal to the number of ways of arranging 3 colors $\{c_1, c_2, c_3\}$ on i places on a circular table considering that we do not have a upper bound on the number of times a color can be used, and that only one color can be placed at a place. have an infinite supply of each color and on each place we can place only 1 color.
Since $\phi(X_i)$ is just like rotating a cycle that has colors on it so be need number of circular permutations only.
Therefore, we need to calculate the number of arrangements of pearls of three colors say $\{R, G, B\}$ on circular string, of size $3, 5, 7$. This is similar to the counting necklaces problem, with the symmetries modified.

- α represents rotation of the 3-sized necklace
- β represents rotation of the 5-sized necklace
- γ represents rotation of the 7-sized necklace

Therefore the group of symmetries S is,

$$S = \{\alpha^i, \beta^j, \gamma^k | i \in [0, 2], j \in [0, 4], k \in [0, 6]\}$$

For $\pi \in S$, we define N_S as,

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

As, seen in the lectures,

$$\text{Number of Permutations} = \sum_S \frac{|N_S|}{|S|}$$

$$\text{Number of Symmetries}(|S|) = 3.5.7 = 105$$

Thus,

$$\text{Number of Permutations} = \frac{1}{105} \sum_S |N_S|$$

Assuming same definition of F_π as seen in the lecture, the set of sequences $\{s | \pi(s) = s, s \in S\}$

$$\text{Number of Permutations} = \frac{1}{105} \sum_{\pi \in S} |F_\pi|$$

Similarly, consider the following, with the similarieties of the 3 sized ring, as isolated the next values will just be multiplications of the rest.

$$|F_0| = 3^3$$

$$|F_\alpha| = 3$$
$$|F_{\alpha^2}| = 3$$

In general for a n sized rind for 3 colors and the i^{th} rotational symmetry (ψ^i)

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

Thus,

$$|F_{\alpha^i\beta^j\gamma^k}| = 3^{gcd(i,3)} \cdot 3^{gcd(j,5)} \cdot 3^{gcd(k,7)}$$

Computation

- $i, j, k \neq 0$ Value, $a_1 = 2 * 4 * 6 * 3^3 = 1296$
- One of i, j, k is 0
  - If $i = 0$, Value, $a_2 = 3^3 * 4 * 6 * 3^2 = 5832$
  - If $j = 0$, Value, $a_3 = 3^5 * 2 * 6 * 3^2 = 26244$
  - If $k = 0$, Value, $a_4 = 3^7 * 2 * 4 * 3^2 = 157464$
- Two of i, j, k are 0,
  - If $i, j = 0$, Value, $a_5 = 3^8 * 6 * 3 = 118098$
  - If $j, k = 0$, Value, $a_6 = 3^{12} * 2 * 3 = 3188646$
  - If $k, i = 0$, Value, $a_7 = 3^{10} * 4 * 3 = 708588$
- $i, j, k = 0$, Value, $a_7 = 3^{15} = 14348907$

The final answer is $\frac{18555075}{105} = \mathbf{176715}$

▷ Which ϕ results in the largest number of colourings?

The **identity permutation** denoted by I, will provide the largest number of colourings. In the identity permutation, all positions are mapped to themselves. This implies that for C_1RC_2, we will have $\phi^j(C_1) = C_2$, which is the same as $C_1 = C_2$, since ϕ is the identity permutation. Thus, all C's will be an unrelated colouring, which is the maximum possible.

Consider any other ϕ, such that this ϕ is not an identity function, this implies that there exists a C_i, such that, $\phi(C_i) = C_j$, and $C_i \neq C_j$. Therefore, C_i is related to C_j, which obviously decreases the number of unrelated permutation.
Therefore, the identity permutation produces the largest number of unrelated colourings.

Question 3

▷ e is transcendental with respect to F_0.

[1]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,

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

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

[1]Alan Baker. *Transcendental Number Theory*. Cambridge University Press, First edition, 1975.

F[α] is a Field

Consider the function ϕ from $F[x]$ to $F[\alpha]$ given by $\phi(f(x)) = f(\alpha)$. Clearly, ϕ is a ring homomorphism. As,

$\phi(f_1(x) + f_2(x)) = \phi(f_1(x)) + \phi(f_2(x))$

Proof. $\phi(f_1(x) + f_2(x)) = f_1(\alpha) + f_2(\alpha) = (f_1(\alpha)) + (f_2(\alpha)) = \phi(f_1(x)) + \phi(f_2(x))$

$\phi(f_1(x).f_2(x)) = \phi(f_1(x)).\phi(f_2(x))$

Proof. $\phi(f_1(x).f_2(x)) = f_1(\alpha).f_2(\alpha) = (f_1(\alpha)) * (f_2(\alpha)) = \phi(f_1(x)).\phi(f_2(x))$

Lemma 3.1: $p(x)$ is irreducible over F.

Proof.
Let's assume $p(x)$ to be reducible. Thus, $p(x)$ can be written as,

$$p(x) = g(x) \times h(x)$$

Where $g(x)$ and $h(x) \in F[x]$ and degree of $g(x)$ and $h(x)$ are less than d.
We know that, F is a field, and since $g(x)$ and $h(x)$ have coefficients in $F[x]$ and $F_0 \in F$, and $\alpha \in$ F, $g(\alpha)$ along with, $h(\alpha) \in F$.
We also know that the additive identity of F is unique.
Since, $p(x)$ is the minimal polynomial of α,

$$p(\alpha) = g(\alpha) \times h(\alpha) = 0$$

This implies either $g(\alpha) = 0$ or $h(\alpha) = 0$.
Thus, we get polynomials in F_0 with degree $< d$ which have α as a root. This contradicts the claim that $p(x)$ is the minimal polynomial. Thus, $p(x)$ is irreducible over F_0.

Lemma 3.2: If $p(x)$ is irreducible then $\langle p(x)\rangle$ is the maximal ideal of F.

Proof.
Let I be any ideal of $F[x]$ such that $\langle p(x)\rangle \subseteq I \subseteq F[x]$.
Since, $I \subseteq F[x], I = \langle g(x)\rangle$. This implies that $p(x) = g(x)h(x)$, but it is known that $p(x)$ is irreducible hence I cannot exist and $p(x)$ is a maximal ideal.

Lemma 3.3: We need to show that $\phi(F[x]) \cong F[x]/\langle p(x)\rangle$.

Proof.
[a]The degree of $p(\alpha) = d$, so each element of $F[x]/\langle p(x)\rangle$ can be writen uniquely in the form

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

as is obvious from the definition of *quotienting* discussed in the lectures.
Also

$$\phi(a_{d-1}x^{d-1} + \cdots + a_0 + \langle p(x)\rangle) = \phi(a_{d-1}x^{d-1} + \cdots + a_0) + \phi(\langle p(x)\rangle)$$

We know $\phi(\langle p(x)\rangle) = 0 \because \langle p(x)\rangle$ is the kernel so we get,

$$\phi(a_{d-1}x^{d-1} + \cdots + a_0 + \langle p(x)\rangle) = \phi(a_{d-1}x^{d-1} + \cdots + a_0)$$

So for each element $t \in [a_{d-1}x^{d-1} + \cdots + a_0]$, we get $\phi(t) = \phi(a_{d-1}x^{d-1} + \cdots + a_0)$
Consider any two polynomials $t_1 \in [P_1], t_2 \in [P_2]$, Here P_1, P_2 are polynomials with

co-efficients form F and degree $\leq d$.

$$\phi(t_1 + t_2) = \phi(t_1) + \phi(t_2)$$
$$= \phi(P_1) + \phi(P_2)$$

Also consider,

$$\phi(t_1 * t_2) = \phi(t_1) * \phi(t_2)$$
$$= \phi(P_1) * \phi(P_2)$$

Consider a map $\psi : \phi(F[x]) \to F[x]/\langle p(x)\rangle$.

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

Consider the following relation,

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

Similarly for the other group operation,

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

Hence ψ is a **Homomorphism**.
Notice that for all such $\phi(f(x))$ that give the same value we will get the same $[P(x)]$ hence ψ is one-one.
Also for each $[P(x)]$ there is at least one $\phi(P(x))$ that maps to it, hence ψ is onto.
$\Rightarrow \psi$ is an isomorphism and $\phi(F[x]) \cong F[x]/\langle p(x)\rangle$

[a] **Reference:** Joseph A. Gallian. *Contemporary Abstract Algebra.* Cengage, Ninth Edition, 2017.

Now, by definition we know that

$$\phi(F[x]) = F[\alpha]$$

This implies that, $F[\alpha] \cong F[x]/\langle p(x)\rangle$, hence $F[\alpha]$ is a field.

▷ The polynomial $x^2 - 5^{1/2^{(j-1)}}$ is irreducible in the ring R_j.

Claim: $x^2 - 5^{1/2^{(j-1)}}$ is irreducible over the ring R_j.

Proof.
Observe that $d = 2^j$ for F_j. We know, $F_0 = a_0$, and, $F_1 = a_0 + a_1(5^{1/2})$. Suppose, $5^{1/4}$ can we written in F_1,

$$a_0 + a_1(5^{1/2}) = 5^{1/4}$$

Shifting the terms and squaring both sides,

$$5(a_1)^2 = (5^{1/4} - a_0)^2 = 5^{1/2} + a_0^2 - 2a_0 5^{1/4}$$
$$5(a_1)^2 = 5^{1/2} + a_0^2 - 2a_0(a_0 + a_1(5^{1/2}))$$
$$5(a_1)^2 + a_0^2 = 5^{1/2}(1 - 2a_0a_1)$$

Now, since the left hand side is positive always, and a rational. The same can be concluded for $(1 - 2a_0a_1)$. This implies that a rational number will be equal to an irrational number, which is not possible. Thus, $x^2 - 5^{1/2}$ does not have a root over, R_1.

Thus, we have proven the specific case for F_1 and F_0.This can be extrapolated to higher powers as well, and this proves that $5^{1/2^{(j)}}$ can't be a part of F_{j-1}.
Thus, since $x^2 - 5^{1/2^{(j-1)}}$ doesn't have a root in F_{j-1}, it is irreducible over $F_{j-1}[x]$.

Additionally, since $5^{1/2^{(j)}} \notin F_{j-1}$, and we find a polynomial that has coefficients in F_{j-1} and irreducible over F_{j-1}, $5^{1/2^{(j)}}$ is an algebraic over F_{j-1}.

▷ $\hat{F}$ is isomorphic of F_j

As proved earlier, if $x^2 - 5^{1/2^{j-1}}$ is irreducible it is a maximal ideal. We know that if if R_j is a ring, $\hat{F} = R_j/I$ is a field for I being the maximal ideal. [Discussed in the Lectures].
We know,

$$\hat{F} \cong F_{j-1}[\alpha_j] = \mathbb{Q}[\alpha_{j-1}][\alpha_j]$$

We need to prove an isomorphism between $\hat{F}$ and F_j. This is equivalent to proving $F_{j-1}[\alpha_j] \cong F_j = \mathbb{Q}[\alpha_j]$ or $F_{j-1}[\alpha_j] \cong \mathbb{Q}[\alpha_j]$. If a bijective function between any $f \in F_{j-1}$ and $q \in \mathbb{Q}$, exists, then we can show that an isomorphism exists, between $\{f_0 + f_1\alpha_j + \cdots | f_0, \cdots \in F_{j-1}\}$ and $\{q_0 + q_1\alpha_j + \cdots | q_0, \cdots \in \mathbb{Q}\}$.

$$f = \{a_0 + a_1\alpha_{j-1} + \cdots | a_0, \cdots \in \mathbb{Q}\}$$

Since, $\alpha = 5^{1/2^{j-1}}$ for $t = 2^{j-1}$, $\alpha^t = 5$, after which the irrational part repeats in a cycle, so the entire f can be rewritten as,

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

Consider $b_i = \frac{n_i}{d_i}$, we can show a **one-one map from F_{j-1} to $\mathbb{Q}$.**, for p_i, q_i are distinct primes.

$$f = \frac{p_1^{n_1} p_2^{n_2} \cdots}{q_1^{d_1} q_2^{d_2} \cdots}$$

We can also define a **one-one map from $\mathbb{Q}$ to F_{j-1}**, such that for $q \in \mathbb{Q}$, each $b_i = q$.
Since, we have a one-one map in both direction so we can form a bijection between F_{j-1} and $\mathbb{Q}$, say δ.
So consider the map $\psi : F_{j-1}[\alpha_j] \to \mathbb{Q}[\alpha_j]$, such that,

$$\psi(\{f_0 + f_1\alpha_j + \cdots | f_0, \cdots \in F_{j-1}\}) = \{\delta(f_0) + \delta(f_1)\alpha_j + \cdots | \delta(f_0), \cdots \in \mathbb{Q}\}$$

This is clearly an isomorphism because δ is a bijection.