CS201A: Midsem Examination

Soham Sammadar 200990 | Akhil Agrawal 200076 | Aditya Tanwar 200057

September 2021

Question 1. (10+10 marks) For any number $\ell > 0$ prove that

$$G_\ell(X) = \sum_{n \geq 0} n^\ell X^n = \frac{g(X)}{(1-X)^{\ell+1}}$$

where $g(X)$ is a polynomial of degree less than ℓ. Using the above, prove that for any numbers k and ℓ, and for any polynomial f of degree at most ℓ,

$$\sum_{i=0}^{\ell+1} (-1)^i \cdot \binom{\ell+1}{i} \cdot f(k+i) = 0$$

<u>**Solution 1.**</u> We assume $\ell \in \mathbb{N}$ and relax the condition on degree of $g(X)$ to be **less than or equal to** ℓ. Also, change the notation for $g(X)$ to be $g_\ell(X)$.

We use induction on ℓ.

Base Case: $\ell = 1$
From the geometric series expansion:

$$\begin{aligned}
\frac{1}{1-X} &= \sum_{i \geq 0} X^i \\
\frac{1}{(1-X)^2} &= \sum_{i \geq 0} iX^{i-1} \quad \text{(Differentiating both sides)} \\
\frac{X}{(1-X)^2} &= \sum_{i \geq 0} iX^i = G_1(X)
\end{aligned}$$

Therefore, $g_1(X) = X$. Indeed, its degree is ≤ 1

Suppose the induction hypothesis holds for $\ell = m \ (\geq 1)$. So we prove the hypothesis for $\ell = m + 1$

Proof.

$$\sum_{n\geq 0} n^m X^n = \frac{g_m(X)}{(1-X)^{m+1}}$$

$$\sum_{n\geq 0} n^{m+1} X^{n-1} = \frac{g_m^{'}(X)(1-X) + g_m(X)(m+1)}{(1-X)^{m+2}} \quad \text{(Differentiating both sides)}$$

$$\sum_{n\geq 0} n^{m+1} X^n = \frac{g_m^{'}(X)(1-X)X + g_m(X)(m+1)X}{(1-X)^{m+2}} = G_{m+1}(X)$$

Also, from the hypothesis, $g_m(X)$ and $g_m^{'}(X)$ have at most m and $(m-1)$ degrees, respectively. Therefore, $g_m(X)(m+1)(X)$ and $g_m^{'}(X)(1-X)(X)$ both have at most $(m+1)$ degree.

Thus, $g_{m+1}(X) = g_m^{'}(X)(1-X)X + g_m(X)(m+1)X$ has degree at most $(m+1)$. We are done with our induction, and consequently the first part of the problem. □

Since ℓ is given as a part of the summation index, we can safely assume it to be a non-negative integer. k is any positive real number.

Lemma 1.1.

$$\sum_{i=0}^{\ell+1} (-1)^\ell \cdot \binom{\ell+1}{i} \cdot i^m = 0 \qquad \forall\, m \in \{0, 1, 2, \ldots, \ell\}$$

Proof. From the previous part we have:

$$G_m(X) = \sum_{n\geq 0} n^m X^n = \frac{g(X)}{(1-X)^{m+1}}$$

where $g(X)$ is a polynomial of degree less than or equal to m. Therefore we have:

$$g(X) = \left(\sum_{n\geq 0} n^m X^n\right)(1-X)^{m+1}$$

$$g(X)(1-X)^{\ell-m} = \left(\sum_{n\geq 0} n^m X^n\right)(1-X)^{\ell+1} \tag{1}$$

Let $H(X) = g(X)(1-X)^{\ell-m}$

Maximum degree of $H(X)$ = Maximum degree of $g(X) + (\ell - m) = m + (\ell - m) = \ell$. Therefore the co-efficient of $X^{\ell+1}$ in $H(X)$ has to be 0.

From R.H.S of equation 1, we obtain the co-efficient of $X^{\ell+1}$ as,

$$\sum_{i=0}^{\ell+1} (-1)^\ell \cdot \binom{\ell+1}{i} \cdot i^m = 0$$

The lemma follows. □

Let $f(x) = \sum\limits_{j=0}^{\ell} a_j x^j$, be an arbitrary polynomial with degree at most ℓ. The given expression is:

$$
\begin{aligned}
&= \sum_{i=0}^{\ell+1} (-1)^i \cdot \binom{\ell+1}{i} \cdot f(k+i) \\
&= \sum_{i=0}^{\ell+1} (-1)^i \cdot \binom{\ell+1}{i} \cdot \left(\sum_{j=0}^{\ell} a_j (k+i)^j \right) \\
&= \sum_{i=0}^{\ell+1} (-1)^i \cdot \binom{\ell+1}{i} \cdot \left(\sum_{j=0}^{\ell} a_j \left(\sum_{p=0}^{j} \binom{j}{p} \cdot k^{j-p} \cdot i^p \right) \right) \quad \text{(Binomial Expansion)} \\
&= \sum_{j=0}^{\ell} a_j \cdot \left(\sum_{p=0}^{j} \binom{j}{p} \cdot k^{j-p} \cdot \sum_{i=0}^{\ell+1} (-1)^i \cdot \binom{\ell+1}{i} \cdot i^p \quad \text{(Rearranging summation signs)} \right) \\
&= \sum_{j=0}^{\ell} a_j \cdot \left(\sum_{p=0}^{j} \binom{j}{p} \cdot k^{j-p} \cdot 0 \right) \quad \text{(From lemma 1.1, as } p \leq \ell) \\
&= \sum_{j=0}^{\ell} a_j \cdot 0 \\
&= 0
\end{aligned}
$$

■

Question 2. (10 marks) Derive the number of primes less than 400 using the principle of Inclusion-Exclusion.

<u>Solution 2.</u> We set up the following notations:

- $n_x :=$ Number of primes less than or equal to x.
- $A(x) :=$ Set of all primes $p \leq x$. $|A(x)| = n_x$.
- $F(a,\ x) :=$ Number of positive integers less than or equal to x and divisible by a.

$$F(a,\ x) = \left\lfloor \frac{x}{a} \right\rfloor$$

- $G(S,\ x) :=$ Number of positive integers less than or equal to x and divisible by every element in set S.

Lemma 2.1. If all elements of set S are pairwise co-prime to each other. Then,

$$G(S,\ x) = \left\lfloor \frac{x}{\prod\limits_{a \in S} a} \right\rfloor$$

Proof. Essentially, $G(S,\ x)$ counts the number of positive integers divisible by the **least common multiple (lcm)**, taken over all elements of S.

$$m := LCM(a) \quad a \in S$$

We can thus, formulate it from $F(a,\ x)$ as follows:

$$G(S,\ x) = F(m,\ x)$$

But as all elements in S are co-prime, their least common multiple is simply their product, $m = \prod\limits_{a \in S} a$. $\square$

For any x, we intend to find the quantity,

$$(x-1) - \bigcup_{p \in A(\lfloor \sqrt{x} \rfloor)} F(p,\ x) + n_{\lfloor \sqrt{x} \rfloor}$$

We briefly discuss each of these terms:

- $(x-1)$: Count of integers between 2 and x (both inclusive). 1 has been excluded because it is neither prime nor composite.
- $\bigcup\limits_{p \in A(\lfloor \sqrt{x} \rfloor)} F(p,\ x)$: Subtracts all integers which are multiples of a prime contained in $A\left(\lfloor \sqrt{x} \rfloor\right)$. However, this subtracts the primes in $A\left(\lfloor \sqrt{x} \rfloor\right)$ too.

- $n_{\lfloor\sqrt{x}\rfloor}$: To compensate for the primes removed by the subtraction of $\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$, we add them back to get the required number of primes.

<u>Claim 1:</u> The quantity $(x-1)-\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$ only accounts for numbers greater than $\sqrt{x}$.

Proof. For any integer $q \leq \sqrt{x}$, there are three cases:

Case 1. $q = 1$: It has been subtracted in the term $(x - 1)$.

Case 2. q is a prime: Since each prime is a multiple of itself, and the term $\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$ subtracts precisely their multiples, thus any prime which is in $A(\lfloor\sqrt{x}\rfloor)$ is removed.

Case 3. q is composite: As q is composite, it will be a multiple of some prime, lesser than itself. Since $q \leq \sqrt{x}$, the prime will be less than $\sqrt{x}$ as well. Thus q will be removed when $\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$ is subtracted.

□

<u>Claim 2:</u> The quantity $(x-1)-\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$ only accounts for primes strictly greater than $\sqrt{x}$.

Proof. We prove that every composite strictly greater than $\sqrt{x}$ has been removed and no prime greater than $\sqrt{x}$ has been removed. For any integer $q > \sqrt{x}$, consider the primes dividing q:

Case 1. There exists at least one prime in $A(\lfloor\sqrt{x}\rfloor)$ which divides q. This implies that q is a multiple of a prime in $A(\lfloor\sqrt{x}\rfloor)$. Hence it must have been removed when $\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$ was subtracted.

Case 2. There exists only one prime which divides q and is not in $A(\lfloor\sqrt{x}\rfloor)$: Obviously, this means that q is a prime. It is not a multiple of any prime in $A(\lfloor\sqrt{x}\rfloor)$, and hence has not been removed under the subtraction.

Case 3. There exists at least two distinct primes dividing q with none of them in $A(\lfloor\sqrt{x}\rfloor)$: Let these two primes be r, s. Therefore $q \geq r\cdot s > \sqrt{x}\cdot\sqrt{x} = x$, a contradiction.

□

Therefore, the term $(x-1)-\bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x)$ accounts for all primes greater than $\sqrt{x}$ and lesser than or equal to x, while $n_{\lfloor\sqrt{x}\rfloor}$ accounts for primes lesser than or equal to $\sqrt{x}$. Adding them gives the total number of primes lesser than or equal to x. So:

$$n_x = (x-1) - \bigcup_{p\in A(\lfloor\sqrt{x}\rfloor)} F(p,\ x) + n_{\lfloor\sqrt{x}\rfloor}$$

and the lemma follows.

Finally, we use the "Principle of Inclusion-Exclusion" to compute $\bigcup\limits_{p \in A(\lfloor \sqrt{x} \rfloor)} F(p,\, x)$. We outline the steps involved, taking $x = 400$:

- $\sqrt{x} = 20 \implies \lfloor \sqrt{x} \rfloor = 20$
- $A(\lfloor \sqrt{x} \rfloor) = A(20) = \{2, 3, 5, 7, 11, 13, 17, 19\}$, and $n_{\lfloor \sqrt{x} \rfloor} = 8$. We also make the key observation that all the elements of $A(20)$ are pairwise co-prime. This property is retained in any subset of $A(20)$ containing more than 2 elements as well.
- By the Principle of Inclusion-Exclusion, we write

$$\bigcup_{p \in A(20)} F(p, 400) = \sum_{i=1}^{i \leq n_{20}} (-1)^{i-1} G(\{a_1, \ldots, a_i \mid a_1 < \cdots < a_i \;\; \& \; a_j \in A(20)\},\, 400)$$

- We simplify the term $G(\{a_1, \ldots, a_i \mid a_1 < \cdots < a_i\},\, 400)$, by using lemma 2.1. Let $S = \{a_1, \ldots, a_i \mid a_1 < \cdots < a_i \;\&\; a_j \in A(20)\}$. As $S \subseteq A$, using lemma 2.1, we write $G(S,\, 400) = \left\lfloor \dfrac{400}{\prod\limits_{a \in S} a} \right\rfloor$.
- It is easy to see that for any $S \subseteq A(20)$, with $|S| \geq 5$, $G(S,\, 400) = 0$. This is because the set $S_0 = \{2, 3, 5, 7, 11\}$, which yields the smallest "lcm" of 2310 among all such S, has $G(S_0,\, 400) = F(2310,\, 400) = 0$.
- The calculations for each term are as follows:
  1. $|S| = 1$, we have $G(S,\, 400) = 580$
  2. $|S| = 2$, we have $G(S,\, 400) = 324$
  3. $|S| = 3$, we have $G(S,\, 400) = 76$
  4. $|S| = 4$, we have $G(S,\, 400) = 3$
  5. $|S| \geq 5$, we have $G(S,\, 400) = 0$
- Using the values above we find that,

$$\bigcup_{p \in A(20)} F(p, 400) = 329$$

- Putting all the terms together, we obtain,

$$n_{400} = (400 - 1) - (329) + (8) = 399 - 329 + 8 = 78$$

Finally, we obtain that the number of primes less than or equal to 400 are $\boxed{\mathbf{78}}$.

■

Question 3. (20 marks) Given a set A, a $\mathbb{Z}$-*module* is defined to be a set whose elements have the form

$$\alpha = \sum_{a \in A} c_a a$$

where $c_a \in \mathbb{Z}$, the set of integers. It is denoted as $\mathbb{Z}(A)$. One can define addition of elements in $\mathbb{Z}(A)$ naturally:

$$\alpha + \beta = \sum_{a \in A} c_a a + \sum_{a \in A} d_a a = \sum_{a \in A} (c_a + d_a) a$$

A proper subset $B \subset \mathbb{Z}(A)$ is called a *submodule* if B is closed under addition, that is, if $\alpha, \beta \in B$ then $\alpha + \beta \in B$. A submodule B is *maximal* if there is no submodule that properly contains B. Prove that $\mathbb{Z}(A)$has a maximal submodule.

Solution 3. Let U be the set of all submodules in $\mathbb{Z}(A)$. Define the subset ($\subseteq$) relation on the elements of U. The relation satisfies all the criteria (namely transitive, reflexive, and anti-symmetric) of a partial order and it also aligns with what needs to be proven. Our aim is to invoke **Zorn's Lemma**. Let C be an arbitrary chain in U. Define T to be the union of all elements in C.

Claim 1: T is an upper bound of C.

Proof. This trivially follows from the definition of T since it is the union of all the elements in C. Hence all elements in C are subsets of T. $\square$

Claim 2: T is closed under addition.

Proof. Suppose $\alpha, \beta \in T$. $\exists$ sets $E, F \in C$ with $\alpha \in E, \beta \in F$. By the total order of C, either $E \subseteq F$ or $F \subseteq E$.

Case 1: $E \subseteq F$

$$\begin{aligned}
&\Rightarrow \alpha, \beta \in F \quad (\text{Since } E \subseteq F) \\
&\Rightarrow \alpha + \beta \in F \quad (\text{Since } F \text{ is a submodule}) \\
&\Rightarrow \alpha + \beta \in T \quad (\text{Since } F \subseteq T)
\end{aligned}$$

Case 2: $F \subseteq E$

$$\begin{aligned}
&\Rightarrow \alpha, \beta \in E \quad (\text{Since } F \subseteq E) \\
&\Rightarrow \alpha + \beta \in E \quad (\text{Since } E \text{ is a submodule}) \\
&\Rightarrow \alpha + \beta \in T \quad (\text{Since } E \subseteq T)
\end{aligned}$$

In both cases, we get $\alpha + \beta \in T$, proving our claim. $\square$

Claim 3: T is a submodule (i.e $T \neq \mathbb{Z}(A)$).

Proof. For the sake of contradiction, suppose $T = \mathbb{Z}(A)$. Define the conjugate of an element $H \in C$ as $\overline{H} = \mathbb{Z}(A) \setminus H$. For two elements $E, F \in C$, it can easily be seen that:

$$E \subseteq F \Leftrightarrow \overline{F} \subseteq \overline{E}$$

By the total order of C, all the conjugate elements of C are also totally ordered - call this new chain $\overline{C}$ (the chain essentially gets reversed). Let $\overline{T}$ be the **intersection** over all the elements in $\overline{C}$.

Case 1: $\overline{T}$ is not empty:

$$\exists \ \alpha \in \overline{T}$$

This implies α belongs to every element in $\overline{C}$. Consequently, α does not belong to any element in C. Hence, T cannot contain α, which is a contradiction since $\alpha \in \mathbb{Z}(A) = T$

Case 2: $\overline{T}$ is empty:
This forces at least one of the elements in $\overline{C}$ to be empty. This is because, by the total ordering of $\overline{C}$, if we take the intersection over some subset of $\overline{C}$, then that intersection set is the minimum element in that subset. Hence,

$$\exists \ \overline{E} \in \overline{C}, \ \overline{E} = \phi$$

By definition then, $E = \mathbb{Z}(A) \setminus \overline{E} = \mathbb{Z}(A)$, a contradiction since:

$$\mathbb{Z}(A) \notin U$$

$$\mathbb{Z}(A) = E \in C \subseteq U$$

$\square$

From claims 2 and 3, we can conclude that $T \in U$. As the relation used ($\subseteq$) is a partial order and every chain of $(U, \subseteq)$ has an upper bound (from claim 1), we can invoke Zorn's Lemma. Thus U has a maximal element. Thus $\mathbb{Z}(A)$ has a maximal submodule.

$\blacksquare$

Initially, we assumed $\mathbb{Z}(A)$ to contain all the possible integer coefficients and came up with a proof accordingly. However, we later thought that $\mathbb{Z}(A)$ is an arbitrary set - and made changes to our proof. The following shows the initial proof that we came up with. There are only changes in the proof of claim 3.

If $\mathbb{Z}(A)$ is allowed to vary over all the possible integer coefficients, a much neater proof to claim 3 can be obtained. We set up some preliminary definitions.

Definition 3.1 (Generator Elements)**.** For any $b \in A$, define $g_{+b} \in \mathbb{Z}(A)$ with the coefficients c_a defined as follows:

$$c_a = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

Define $g_{-b} \in \mathbb{Z}(A)$ similarly:

$$c_a = \begin{cases} -1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

These elements are called the **Generator Elements**.

Definition 3.2 (Generator Set)**.** Define G, the **Generator Set** as:

$$G = \bigcup_{b \in A} \{g_{+b},\ g_{-b}\}$$

Lemma 3.1. A set which is a superset to G and closed under addition is equal to $\mathbb{Z}(A)$.

Proof. For any $\alpha \in \mathbb{Z}(A)$ such that:

$$\alpha = \sum_{a \in A} c_a a$$

We can produce each coefficient c_a from the sum of elements in G, individually, as follows:

$$c_a a = \begin{cases} \sum_{i=1}^{c_a} g_{+a} & \text{if } c_a > 0 \\ \sum_{i=1}^{|c_a|} g_{-a} & \text{if } c_a < 0 \\ g_{+a} + g_{-a} & \text{if } c_a = 0 \end{cases}$$

Hence we can generate any element $\alpha \in \mathbb{Z}(A)$. □

Now we prove claim 3.

Proof. For the sake of contradiction, suppose $T = \mathbb{Z}(A)$. Then all the generator elements belong to T. Hence each of the generator elements belong to some element in C. But, by the total order of C, as we move up the chain, the generator elements "pile up". Hence, at one point along the chain, we get an element E which is a superset to G. But by lemma 3.1, E is equal to $\mathbb{Z}(A)$, which is a contradiction since

$$\mathbb{Z}(A) \notin U$$

$$\mathbb{Z}(A) = E \in C \subseteq U$$

□

We can proceed as earlier.