Individual Finals B Solution

1. For a binary string S (i.e. a string of 0's and 1's) that contains at least one 0, we produce a binary string $f(S)$ as follows:

   - If the substring 110 occurs in S, replace each instance of 110 with 01 to produce $f(S)$;
   - Otherwise, replace the leftmost occurrence of 0 in S by 1 to produce $f(S)$.

   Given binary string S of length n, we define the *lifetime* of S to be the number of times f can be applied to S until the resulting string contains no more 0's. For example,

   $$111000 \to 10100 \to 11100 \to 1010 \to 1110 \to 101 \to 111$$

   so the lifetime of 111000 is 6. For a given $n \geq 2$, which binary string(s) of length n have the longest lifetime?

   Proposed by Austen Mazenko

   Solution: Let $g(S) = \#\{0\text{'s in } S\} + \#\{\text{length of } S\}$. Importantly, $g(f(S)) \leq g(S) - 1$: applying f to S will decrease its g-value by at least 1. If we replace 110 by 01 in the string, k times, then $g(S)$ decreases by k, and if we replace 0 by 1, $g(S)$ decreases by 1.
   Claim: Applying f to $S = 00...0$, m times, will decrease the g-value by *exactly* m.
   Proof: The only 'forms' of strings we can get from applying f repeatedly are 00...00, 100..00, 1100...00, and 0100...00. Applying f to any of these forms will bring you to another form. The only time we decrease g by 2 or more, is when we change 110 to 01 in 2 or more spots in the string, which never happens among these forms. So, g decreases by 1 every time.

   Once we have this, $S_n = 00...00$ (n zeros) has the highest initial g-value (of $2n$), and only decreases by 1 each time. Its final g-value is at most 2 (since all of its possible 'forms' have at most 2 1's in it). Note that any string of length ≥ 2 can never change into the string '1' after applications of f. So, S_n has the highest possible initial g-value out of all length-n strings, has the lowest possible final g-value, and its g-value decreases the slowest, so its lifetime must be maximal, and its lifetime is $2n - 2$ (its g value decreases from $2n$ to 2, decreasing by exactly 1 under every application of f).

2. Let f be a polynomial with degree at most $n - 1$. Show that

   $$\sum_{k=0}^{n} \binom{n}{k} (-1)^k f(k) = 0.$$

   Proposed by Ben Zenker, solved by Atharva Pathak

   Solution: It suffices to show this for the polynomials

   $$f(X) = X(X-1)\cdots(X-\ell+1)$$

   for $0 \leq \ell \leq n-1$, since all other polynomials of degree at most $n-1$ can be written as finite linear combinations of them. We have

$$\begin{aligned}
&\sum_{k=0}^{n} \binom{n}{k} (-1)^k \cdot k(k-1)\cdots(k-\ell+1) \\
&= \sum_{k=\ell}^{n} \frac{n!}{k!(n-k)!} (-1)^k \cdot k(k-1)\cdots(k-\ell+1) \\
&= \sum_{k=\ell}^{n} \frac{n!}{(k-\ell)!(n-k)!} (-1)^k \\
&= \frac{(-1)^\ell n!}{(n-\ell)!} \sum_{k=\ell}^{n} \frac{(n-\ell)!}{(k-\ell)!(n-k)!} (-1)^{k-\ell} 1^{n-k} \\
&= \frac{(-1)^\ell n!}{(n-\ell)!} (-1+1)^{n-\ell} \\
&= 0,
\end{aligned}$$

as desired.

3. Let $p > 3$ be a prime and $k \geq 0$ an integer. Find the multiplicity of $X-1$ in the factorization of

$$f(X) = X^{3p^k-1} + X^{3p^k-2} + \cdots + X + 1$$

modulo p; in other words, find the unique non-negative integer r such that $(X-1)^r$ divides $f(X)$ modulo p, but $(X-1)^{r+1}$ does not divide $f(X)$ modulo p.

Proposed by Michael Cheng and Steven Wang

Solution: First note

$$f(X) = \frac{X^{3p^k} - 1}{X - 1}.$$

The key trick is to make the substitution $X = Y + 1$, so we are instead looking for the multiplicity of Y in

$$f(Y) = \frac{(Y+1)^{3p^k} - 1}{Y}.$$

Now

$$(Y+1)^{3p^k} = \sum_{\ell=0}^{3p^k} \binom{3p^k}{\ell} Y^\ell,$$

and we claim the coefficient $\binom{3p^k}{\ell}$ is divisible by p unless $p^k \mid \ell$.

We use the notation

$$v_p(n) = \{k \in \mathbb{Z}_{\geq 0} : p^k \mid n \text{ and } p^{k+1} \nmid n\}.$$

It is well-known that

$$v_p(n!) = \sum_{r=0}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor.$$

Therefore

$$v_p\left(\binom{3p^k}{\ell}\right) = v_p\left(\frac{(3p^k)!}{\ell!(3p^k-\ell)!}\right) = \sum_{r=0}^{\infty} \underbrace{\left(\left\lfloor \frac{3p^k}{p^r} \right\rfloor - \left\lfloor \frac{\ell}{p^r} \right\rfloor - \left\lfloor \frac{3p^k-\ell}{p^r} \right\rfloor\right)}_{S_r}.$$

We have three cases depending on r:

- $r > k$: then all three floor functions are 0 (here we used the assumption that $p > 3$), so $S_r = 0$.
- $r \le k$: then $p^r \mid 3p^k$, so $S_r \ge 0$. More careful analysis shows that $S_r = 0$ iff $p^r \mid \ell$.

Therefore, $v_p\left(\binom{3p^k}{\ell}\right) = 0$ iff $p^k \mid \ell$. Thus, modulo p, we have

$$\begin{aligned} f(Y) &= \frac{(Y+1)^{3p^k} - 1}{Y} \\ &= \frac{1}{Y}\left[\sum_{\ell=0}^{3p^k} \binom{3p^k}{\ell} Y^\ell - 1\right] \\ &\equiv \frac{1}{Y}\left(Y^{3p^k} + AY^{2p^k} + AY^{p^k}\right) \qquad A = \binom{3p^k}{2p^k} = \binom{3p^k}{p^k} \\ &= Y^{3p^k-1} + AY^{2p^k-1} + AY^{p^k-1}, \end{aligned}$$

and $p \nmid A$, so the answer is $\boxed{p^k - 1}$.

Remark. The $X = Y + 1$ trick can be used to prove the cyclotomic polynomial $\Phi_{p^k}(X) = X^{p-1} + \cdots + X + 1$ is irreducible over $\mathbb{Z}$. In fact, one can check that $\Phi_{p^k}(Y+1)$ satisfies the Eisenstein criterion.