Problem Tutorial: "Div"

Multiply both sides by $(x-1)$. We need to count $x > 1$ such that $P_0(x) = d_0 x^{b_0} + d_1 x^{b_1} + \ldots + d_{k-1} x^{b_{k-1}}$ is divisible by $x^m - 1$ (check $x = 1$ separately).

Taking $P_0(x)$ modulo $x^m - 1$ as a polynomial, we'll get $P(x) = d_0 x^{b_0 \bmod m} + d_1 x^{b_1 \bmod m} + \ldots + d_{k-1} x^{b_{k-1} \bmod m}$. If $P(x) \equiv 0$, the answer is infinite. Otherwise, let's count $x > 1$ such that $P(x)$ is divisible by m.

Let's rewrite $P(x)$ as $P(x) = e_0 + e_1 x + \ldots + e_{m-1} x^{m-1}$. Note that if $x > \max(|e_0|, |e_1|, \ldots, |e_{m-1}|) + 1$, then $P(x) \neq 0$ and $|e_0| + |e_1 x| + \ldots + |e_{m-1}| x^{m-1} < x^m - 1$, therefore, we don't need to consider such x. Now we only need to consider $O(n)$ values of x.

Let's fix x and transform $P(x)$ as follows:

- if there's some i such that $e_i \geq x$, subtract x from e_i and add 1 to $e_{(i+1) \bmod m}$;
- if there's some i such that $e_i \leq -x$, add x to e_i and subtract 1 from $e_{(i+1) \bmod m}$;
- otherwise, stop the process.

This transformation keeps the value of $P(x)$ the same. Each step decreases the sum of $|e_i|$ by at least $x - 1$, therefore we'll do $O(\frac{n}{x})$ steps.

After this process, we have $|e_i| < x$ for all i, and $P(x)$ is divisible by $x^m - 1$ if one of the following applies: all $e_i = 0$, all $e_i = x - 1$, or all $e_i = -x + 1$.

We can perform all steps efficiently using built-in associative containers with $O(\log n)$ overhead and rollback changes done for some x before proceeding to the next x. Since there are $\sum_{x=2}^{n} O(\frac{n}{x}) = O(n \log n)$ steps to be done, the overall time complexity is $O(n \log^2 n)$.