Exponential of a series.

In this problem, all power series we consider will have coefficients in \( \mathbb{Q} \); all complexity estimates will count operations in \( \mathbb{Q} \) at unit cost. You can reuse all results seen or used in class on the function \( M \), such as

\[
M(n), \quad M(n+1) = O(M(n)), \quad M(2n) = O(M(n)), \quad M(1)+M(2)+\cdots+M(2^k) = O(M(2^k)), \quad \ldots, 
\]
as well as the results on the cost of power series inversion.

1. Suppose that \( f \) is a power series of the form

\[
f = f_1 x + f_2 x^2 + f_3 x^3 + \cdots, 
\]

so that \( f_0 = 0 \). Prove that the coefficients of \( x^0, x^1, \ldots, x^{n-1} \) in \( f^n \) are zero.

*In all this problem, we will use such an \( f \).*

2. We now define

\[
i(f) = 1 - f + f^2 + \cdots + (-1)^n f^n + \cdots \\
\ell(f) = f - \frac{f^2}{2} + \frac{f^3}{3} + \cdots + (-1)^{n-1} \frac{f^n}{n} + \cdots \\
\exp(f) = 1 + f + \frac{f^2}{2!} + \frac{f^3}{3!} + \cdots + \frac{f^n}{n!} + \cdots 
\]

We admit that all these power series are well-defined. You should imagine that \( \exp(f) \) is the exponential of \( f \) and that \( \ell(f) \) is the logarithm of \( 1 + f \).

(a) Compute \( \exp(x + 2x^2 + 1000x^3) \mod x^3 \)

(b) Question (1) implies that \( f^n \mod x^n = 0 \), but also \( f^{n+1} \mod x^n = 0, f^{n+2} \mod x^n = 0, \ldots \) (this is easy; I don’t ask you to prove it). Use this to give a (naive) algorithm that computes \( \exp(f) \mod x^n \) in \( O(nM(n)) \) operations.

The goal of this problem is to compute \( n \) terms of \( \exp(f) \) more efficiently; we will first show how to compute \( n \) terms of \( \ell(f) \).
3. Prove that \( i(f) = 1/(1 + f) \), by proving that \((1 + f)i(f) = 1\). Using Newton iteration, how many operations does it take to compute \( n \) terms of \( i(f) \)?

4. Let \( f' \) be the derivative of \( f \) with respect to \( x \). If
\[
f = f_1x + f_2x^2 + f_3x^3 + \cdots,
\]
what does \( f' \) look like?

5. Prove that the derivative of \( \ell(f) \) with respect to \( x \) is \( f'i(f) \). Deduce that you can compute \( n \) terms of \( \ell(f) \) in \( O(M(n)) \) operations.

**Hint:** \((f^k)' = kf'f^{k-1}\). **You can freely use term-wise differentiation without justifying it.**

6. We will admit that
\[
\ell(\exp(f) - 1) = f.
\]
I’m not asking for a proof; instead, verify that, for \( f = x \),
\[
\ell(\exp(x) - 1) \text{ rem } x^4 = x.
\]

7. If we write \( g = \exp(f) - 1 \), then the previous equality shows that
\[
\ell(g) - f = 0.
\]
Show that the Newton iteration for this equation (when \( g \) is the unknown to solve for) is
\[
g_{(i+1)} = g_{(i)} - (g_{(i)} + 1)(\ell(g_{(i)}) - f) \mod x^{2i+1}.
\]
**You don’t have to prove correctness of the iteration. You can start by explaining why the derivative of \( \ell(g) \) with respect to \( g \) should be \( 1/(1 + g) \).**

8. Taking correctness for granted, prove that you can compute \( n \) terms of \( \exp(f) \) in \( O(M(n)) \) operations.