MATH 467 FACTORIZATION AND PRIMALITY, FALL TERM 2024, PROBLEMS 1

Return by Wednesday 4th September

For elements of $\mathbb{Z}$ we use the notation $a|b$ to mean that there is a $c \in \mathbb{Z}$ such that $b = ac$.

1. Let $n \in \mathbb{Z}$ and $m \in \mathbb{Z}$ with $0 \le m \le n$. The binomial coefficient $\binom{n}{m}$ is defined inductively by

$$\binom{0}{0} = 1, \quad \binom{n}{-1} = 0, \quad \binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$$

(i) Prove that $\binom{n}{m} \in \mathbb{N}$.
(ii) Prove that if p is a prime and $1 \le m \le p-1$, then $p | \binom{p}{m}$.

2. Prove that no polynomial $f(x)$ of degree at least 1 with integral coefficients can be prime for every positive integer x.

3. If $2^n + 1$ is an odd prime for some integer n, prove that n is a power of 2.

4. Prove that every positive integer is uniquely expressible in the form

$$2^{j_0} + 2^{j_1} + 2^{j_2} + \cdots + 2^{j_m}$$

where $m \ge 0$ and $0 \le j_0 < j_1 < j_2 < \cdots < j_m$.

5. Prove that there are no positive integers a, b, n with $n > 1$ such that

$$(a^n - b^n) | (a^n + b^n).$$

6. Write a program to evaluate the expression $a^m \pmod{m}$ when $a = 2$ or 3 and m is
(i) 2447952037112100847479213118326022843437705003126287, or
(ii) 59545797598759584957498579859585984759457948579595794859456799501.
A copy of your program should be submitted with your solutions to gain credit.