1. In the first class we proved that there are infinitely many primes. This problem asks for an alternative proof. Let \( a_n = 2^{2^n} + 1 \). Prove that for any positive integer \( k \) we have \( \prod_{j=0}^{k-1} a_j = a_k - 2 \), and then explain why this implies that there are infinitely many primes (hint: Induction).

2. (a) Prove that the equation \( x^2 + y^2 + z^2 = 999 \) has no integer solutions (hint: eight is a nice number).

(b) Let \( n \) be a positive integer and denote its digits from right to left as \( d_0, d_1, \ldots, d_k \) (that is, if \( n = 157 \) then \( d_0 = 7, d_1 = 5, \) and \( d_2 = 1 \)). Prove that \( 11 \mid n \) if and only if \( \sum_{i=0}^{k} (-1)^i d_i \) (that is, \( d_0 - d_1 + d_2 - \cdots \)) is divisible by 11.

3. Let \( m \) and \( n \) be relatively prime positive integers. Express \( \varphi(mn) \) in terms of \( \varphi(m) \) and \( \varphi(n) \). Prove your answer.

4. Adam would like to perform an online purchase of 100 pineapples from Prof. Nets Katz. He wants to verify that the person that he is in contact with is indeed Nets. Nets’ public key (from the RSA algorithm) is available online to everyone, and if Nets would send Adam his private key then Adam would be able to verify that the two keys indeed fit (that is, \( de \equiv 1 \mod \phi(n) \)). Obviously Nets does not wish to give Adam his private key, since then it would no longer be private. How can Nets still convince Adam that he has the real private key? Explain why your solution works. (Generating a new private key is not allowed. Use only the existing keys.)

5. Take two arbitrary composite odd numbers with at least four digits (for example, use \texttt{www.wolframalpha.com} to generate a random number and to verify that it is not a prime). One of the numbers must be congruent to 1 mod 4, and the other must be congruent to 3 mod 4. Find a composite witness for each of the two numbers (witnesses of the same type as in the Miller-Rabin algorithm).