56) Let \( p \) be prime with \( p \equiv 3 \pmod{4} \) and let \( q = 2p + 1 \).
   
a) Show that if \( q \) is prime, we have that \( q | 2^p - 1 \). (Hint: Evaluate \( 2^{\frac{q-1}{2}} \pmod{q} \).)
   
b) Show (without using a computer) that \( 2^{50051} - 1 \) is composite.

57) For \( n \in \{10^3, 10^4, 10^5, 10^6\} \) determine the smallest value \( m \) such that there is a probability \( p > \frac{1}{2} \) that (at least) two out of \( m \) random integers in the range \( [0..n-1] \) are equal.

58) Factorize 9374251 using Pollard's \( \rho \)-method (you do not need to group differences for Gcd calculations).
   You may use a computer for modulo arithmetic and for computing geds and \texttt{IsPrime} for primality tests.
   In GAP it might be convenient to use 
   \texttt{CTRL-P} to get previous lines back or to write a small \texttt{for}-loop. You can use \texttt{LogTo} to obtain a transcript file.

59) We consider the drawing of random elements (with repetition) from a set of \( p \) elements. Suppose that the first repeated drawing occurs with the \( m \)-th \( (m \geq 2) \) draw.
   
a) Using the inequality \( 1 - x \leq e^{-x} \), show that for \( j \geq 2 \), the probability
      \[
      \text{prob}(m \geq j) \leq \prod_{1 \leq i < j} e^{-(i-1)/p} \leq e^{-(j-2)^2/2p}.
      \]
      b) The expected value for the number of choices \( m \) is defined as:
      \[
      \mathcal{E}(m) = \sum_{j \geq 2} j \cdot \text{prob}(m = j) = \sum_{j \geq 2} \text{prob}(m \geq j)
      \]
      (you do not need to show this). Show that:
      \[
      \mathcal{E}(m) \leq 1 + \int_{0}^{\infty} e^{-x^2/2p} \, dx \leq 1 + \sqrt{2p} \int_{0}^{\infty} e^{-x^2} \, dx
      \]
      (Hint: Riemann sum and substitution)
      c) Assuming that the function \( f(x) = x^2 + 1 \) produces random values, show that there is a constant \( c \) such that Pollard’s \( \rho \) method will take in average \( c \sqrt{p} \) steps to find a prime factor \( p \).

60\*) Why isn’t it a good idea to use the functions \( f(x) = ax + b \) (for \( a, b \in \mathbb{Z} \)) or \( f(x) = x^2 \) in Pollard’s \( \rho \) method? Explain.

Problems marked with a * are bonus problems for extra credit.