Please print your name:

No notes, calculators or tools of any kind are permitted. There are 40 points in total. You need to show work to receive full credit.

## Good luck!

**Problem 1.** (7+1 points) Eve intercepts the ciphertext  $c = (111\ 111\ 000)_2$ . She knows it was encrypted with a stream cipher using the linear congruential generator  $x_{n+1} \equiv 5x_n + 1 \pmod{8}$  as PRG.

- (a) Eve also knows that the plaintext begins with  $m = (010 \ 1...)_2$ . Break the cipher and determine the plaintext.
- (b) Eve was able to crack the ciphertext because the PRG is lacking a property that is crucial for cryptography. Which property is that?

## Problem 2. (4 points)

(a) Suppose $N$ is composite. $x$ is a Fermat liar modulo $N$ if and only if	
(b) 7 (mod 10) $\square$ is a Fermat liar because	]
(scratch space: show your work for partial credit)	

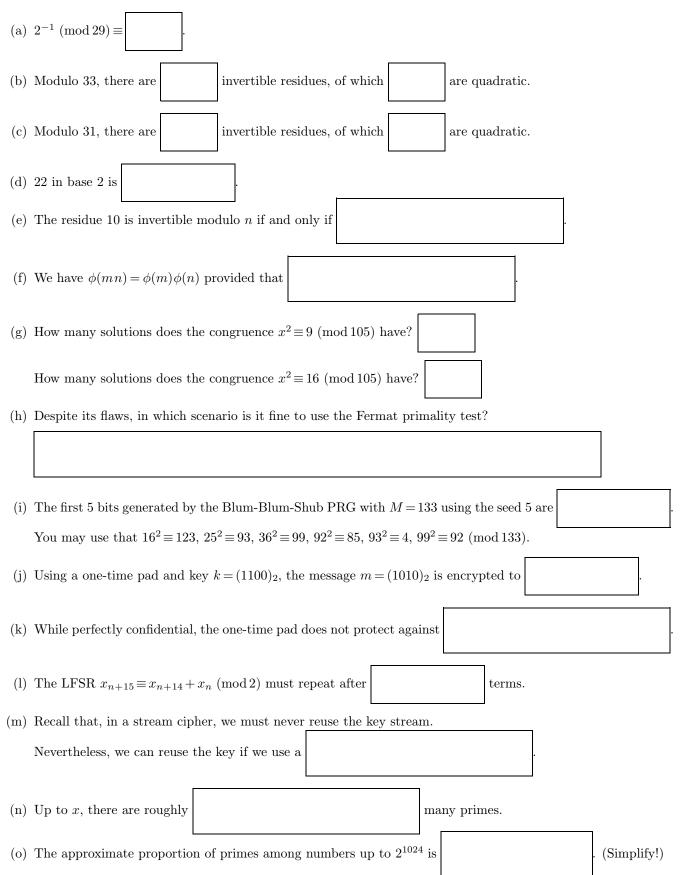
**Problem 3.** (6 points) Using the Chinese remainder theorem, determine all solutions to  $x^2 \equiv 4 \pmod{55}$ .

Problem 4. (5 points) Evaluate  $40^{16011} \pmod{34}$ .

Show your work!

Problem 5. (2 points) Briefly outline the Fermat primality test.

Problem 6. (15 points) Fill in the blanks.



(extra scratch paper)