Math/CS 6A, Problem Set 2

1. Find all solutions to the equation $35x \equiv 10 \mod 50$.

2. Find all integers that leave remainders 1, 2, and 3 when divided by 9, 8, and 7, respectively.

3. Prove that if an odd integer $n > 1$ is not a prime or a prime power, then there exists a nontrivial square root of 1 modulo n.

4. A message has been encrypted using RSA and the encoding $01 \leftrightarrow A$, $02 \leftrightarrow B$, $\ldots$, $26 \leftrightarrow Z$ with exponent $e = 5$ and modulus $n = 2881$. The encrypted message is

$$2688\ 0559\ 0752\ 0915\ 2112\ 0564\ 2743\ 2783.$$

What is the decrypted message?

5. The number 1288119601 is composite. Find a Miller–Rabin witness for this fact.