1. This problem will explore the difficulty of factoring a number $m$ (e.g. a modulus used in an RSA public key) by brute force.

   (a) Suppose that Eve attempts to factor $m$ by trying possible divisors until she finds one that divides $m$. She does this as follows:

   - She uses 10 billion computers (a bit more than one for each person on Earth).
   - Each computer can test 1 billion possible divisors every second.
   - She runs each computer for $10^{18}$ seconds (this is slightly longer than twice the age of the universe).

   In order to be sure to factor $m$, Eve needs to test roughly $\sqrt{m}$ different possible divisors. What is the largest possible $m$ that Even could factor in this way? Your answer need not be exact; a rough approximation is fine.

   (b) A typical implementation of RSA encryption uses 1024-bit keys, meaning that the modulus used is roughly $2^{1024}$. How close would Eve's attack (described above) come to factoring such a modulus?

   *Note.* In 1991, RSA Laboratories published a list of numbers of various sizes, all a product of two primes, and used to offer cash prizes to anyone who could factor them. The longest such number ever factored was 768 bits long, and was factored by a bank of computers over the course of two years from 2007 to 2009. This computation used a method called the *general number field sieve*, which is much more efficient than the brute-force attack described above.

2. (a) Find a solution to the following problem, from Sun Tzu's Mathematical Manual (circa 300 C.E.): "We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"

   (b) Find a solution between 100 and 200 to the problem in part (a).

3. Suppose that Bob's RSA public key is $(9797, 211)$. This means that, in order to encrypt a secret $s$ (between 0 and 9796, inclusive), Alice computes the remainder when $s^{211}$ is divided by 9797. Determine Bob's decrypting exponent (private key).

   *Hint.* The number 9797 is divisible by 97.

4. Compute the remainder when $11^{21}$ is divided by 29.

5. Determine the last two digits (tens digit and units digit) of $3^{13^{2015}}$.

6. Find the smallest integer $n$ such that the last two digits of $n^3$ are "77."

   *Hint.* Use the Chinese Remainder Theorem to express the problem as two different congruences with different moduli, and solve these one at a time.