1. Given $A = 1595022$ and $B = 150$. [15 pts]
   (a) Find the prime factorizations of $A$ and $B$ and use them to find $\gcd (A, B)$.
   (b) Find $\gcd (A, B)$ using the Euclidean Algorithm.

2. Use the Chinese Remainder Theorem to find the smallest and second smallest nonnegative solutions to the system: [15 pts]
   
   $x \equiv 2 \mod 11$
   $x \equiv 6 \mod 23$
   $x \equiv 2 \mod 3$

3. For each of $n = 39, 774, 1544, 21214$ find the exact value $p_n$ of the $n^{th}$ prime (however you want) and then approximate value $a_n$ of the $n^{th}$ prime (using the Prime Number Theorem Corollary). Calculate the percentage error
   
   $\frac{100|p_n - a_n|}{p_n}$

   for each.

4. Find all incongruent solutions mod 135 to the linear system: [10 pts]

   $115x \equiv 60 \mod 135$

5. Find all primitive roots for $n = 17$ as follows: First find the smallest positive primitive root. Then use the Theorem from class which yields all the remaining ones. Final answers should be least nonnegative residues. [15 pts]

6. It’s a fact that $r = 11$ is a primitive root mod 17. [15 pts]
   (a) Use this to construct a table of indices for this primitive root.
   (b) Use the table of indices to solve the equation: $x^{14} \equiv 8 \mod 17$. Your answer(s) should be mod 17.
   (c) Use the table of indices to solve the equation: $9^x \equiv 8 \mod 17$. Your answer(s) should be mod 16.

7. Calculate the following Jacobi symbols: [15 pts]
   (a) $\left(\frac{1251}{997}\right)$
   (b) $\left(\frac{1251}{50431}\right)$
8. Suppose you intercept the following ciphertext from Alice to Bob: \[ 13215 \ 2145 \ 11599 \ 1590 \ 4270 \ 13403 \ 6883 \ 20025 \ 9715 \]

You know that Bob’s public key is \((e, n) = (1267, 24613)\). Bob thinks this is secure because he doesn’t believe that his \(n\) can be factored easily. Factor \(n = 24613\), find \(\phi(n)\), find \(d\) and then decrypt the message. Be clear about the steps you take.

9. Determine if each of the following sets is well-ordered. If a set is not well-ordered give evidence. \[ 15 \text{ pts} \]
   If a set is well-ordered no evidence is required.
   (a) \( 4\mathbb{Z} \)
   (b) \( \{0, \frac{1}{5}, \frac{1}{27}, \ldots \} \)
   (c) \([0, \infty) \cap 2\mathbb{Z}\)

10. Suppose \(p \geq 37\) is an unknown prime. Find all solutions to \(x^2 + 32 \equiv 12x \mod p\). Note that your solutions will be \(\mod p\).

11. Consider the inequality:

\[ 5^n < n! \]

   (a) Find the smallest positive integer \(n_0\) for which this is true. Do this however you wish.
   (b) Prove by induction that \(5^n < n!\) for all \(n \geq n_0\).

12. Suppose \(p\) is an odd prime such that there is some \(a\) so that \(a\) is a quadratic residue of \(p\) but \(2a\) is a quadratic non-residue of \(p\). Prove that \(p \equiv \pm 3 \mod 8\).

13. Prove that for \(a, b \in \mathbb{Z}\) and \(n \in \mathbb{Z}^+\) that if \(a^n \mid b^n\) then \(a \mid b\).

14. Prove that if \(a, b, c \in \mathbb{Z}\) with \(\gcd(a, b) = 1\) and \(c \mid (a + b)\) then \(\gcd(c, a) = \gcd(c, b) = 1\).