1. Given $A = 9388743$ and $B = 9018009$. \[15 \text{ pts}\]
   (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:

\[
\begin{align*}
    x &\equiv 9 \pmod{16} \\
    x &\equiv 5 \pmod{9} \\
    x &\equiv 5 \pmod{19}
\end{align*}
\]

3. For each of $n = 55, 340, 6459, 62306$ find the exact value $p_n$ of the $n^{\text{th}}$ prime (however you want) and then approximate value $a_n$ of the $n^{\text{th}}$ prime (using the Prime Number Theorem Corollary). Calculate the percentage error

\[
100 \frac{|p_n - a_n|}{p_n}
\]

for each.

4. Find all incongruent solutions mod 126 to the linear system:\[10 \text{ pts}\]

\[
60x \equiv 48 \pmod{126}
\]

5. Find all primitive roots for $n = 23$ 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.

6. It’s a fact that $r = 10$ is a primitive root mod 19. \[15 \text{ pts}\]
   (a) Use this to construct a table of indices for this primitive root.
   (b) Use the table of indices to solve the equation: $x^{16} \equiv 11 \pmod{19}$. Your answer(s) should be mod 19.
   (c) Use the table of indices to solve the equation: $5^x \equiv 11 \pmod{19}$. Your answer(s) should be mod 18.

7. Calculate the following Jacobi symbols:\[15 \text{ pts}\]
   (a) $\left( \frac{1863}{1073} \right)$
   (b) $\left( \frac{1863}{3551} \right)$
8. Suppose you intercept the following ciphertext from Alice to Bob:

\[ 19795 \ 23197 \ 24632 \ 22236 \ 22918 \ 20374 \ 6049 \ 15038 \]

You know that Bob’s public key is \((e, n) = (1873, 26989)\). Bob thinks this is secure because he doesn’t believe that his \(n\) can be factored easily. Factor \(n = 26989\), 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.
   If a set is well-ordered no evidence is required.
   \[ \begin{align*}
   & (a) \ \{0, \frac{1}{4}, \frac{1}{16}, \frac{1}{64}, \ldots\} \\
   & (b) \ 3\mathbb{Z} \\
   & (c) \ \{0\} \cup \left\{ \frac{n}{n+4} \mid n \in \mathbb{Z}^+ \right\}
   \end{align*} \]

10. Suppose \(p \geq 29\) is an unknown prime. Find all solutions to \(x^2 + 24 \equiv 10x \mod p\). Note that your solutions will be mod \(p\).

11. Consider the inequality:

\[ 6^n < n! \]

   (a) Find the smallest positive integer \(n_0\) for which this is true. Do this however you wish.
   (b) Prove by induction that \(6^n < n!\) 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 \((c, a) = \gcd(c, b) = 1\).