1. Given $A = 115934$ and $B = 109850$. [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]

\[
x \equiv 2 \pmod{8} \\
x \equiv 6 \pmod{17} \\
x \equiv 11 \pmod{15}
\]

3. For each of $n = 31, 583, 4279, 87535$ 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

\[
100 \left| p_n - a_n \right| / p_n
\]

for each.

4. Find all incongruent solutions mod 90 to the linear system: [10 pts]

\[
25x \equiv 25 \pmod{90}
\]

5. Find all primitive roots for $n = 29$ 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 $r = 8$ is a primitive root mod 11. [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: $x^2 \equiv 3 \pmod{11}$. Your answer(s) should be mod 11.

(c) Use the table of indices to solve the equation: $5^x \equiv 3 \pmod{11}$. Your answer(s) should be mod 10.

7. Calculate the following Jacobi symbols: [15 pts]

(a) \( \left( \frac{1555}{29235} \right) \)

(b) \( \left( \frac{1555}{29235} \right) \)
8. Suppose you intercept the following ciphertext from Alice to Bob:

\[
7145\ 7876\ 7017\ 11164\ 11819\ 8593\ 4143\ 2847\ 5911\ 9190
\]

You know that Bob’s public key is \((e, n) = (1967, 13231)\). Bob thinks this is secure because he doesn’t believe that his \(n\) can be factored easily. Factor \(n = 13231\), 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.

   (a) \(\{0, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots\}\)

   (b) \(\{1\} \cup \left\{\frac{n+3}{n} \mid n \in \mathbb{Z}^+\right\}\)

   (c) \(\left\{\lfloor \sqrt{n} \rfloor \mid n \in \mathbb{Z}^+\right\}\)

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:

\[4^n < n!\]

   (a) Find the smallest positive integer \(n_0\) for which this is true. Do this however you wish.

   (b) Prove by induction that \(4^n < n!\) 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 \(a^n | b^n\) then \(a | b\).

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