1. Given $A = 14395668628575$ and $B = 11455899580125$. \[15\text{ pts}\]
   (a) Find the prime factorizations of $A$ and $B$ and use them to find $\text{gcd} (A, B)$.
   (b) Find $\text{gcd} (A, B)$ 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 18 \mod 23 \\
   x &\equiv 5 \mod 30 \\
   x &\equiv 10 \mod 29
   \end{align*}

3. For each of $n = 75, 987, 9487, 79798$ 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

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

   for each.

4. Find all incongruent solutions mod 91 to the linear system: \[10\text{ pts}\]

   \[28x \equiv 49 \mod 91\]

5. Find all primitive roots for $n = 31$ 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. \[15\text{ pts}\]

6. It’s a fact that $r = 12$ is a primitive root mod 17. \[15\text{ pts}\]
   (a) Use this to construct a table of indices for this primitive root.
   (b) Use the table of indices to solve the equation: $x^2 \equiv 2 \mod 17$. Your answer(s) should be mod 17.
   (c) Use the table of indices to solve the equation: $9^x \equiv 2 \mod 17$. Your answer(s) should be mod 16.

7. Calculate the following Jacobi symbols: \[15\text{ pts}\]
   (a) \(\left(\frac{1227}{9487}\right)\)
   (b) \(\left(\frac{1227}{36859}\right)\)
8. Suppose you intercept the following ciphertext from Alice to Bob:

\[\begin{align*}
7036 & \quad 10594 & \quad 10957 & \quad 10594 & \quad 12341 & \quad 9800 & \quad 3238 & \quad 6921
\end{align*}\]

You know that Bob’s public key is \((e, n) = (1113, 22663)\). Bob thinks this is secure because he doesn’t believe that his \(n\) can be factored easily. Factor \(n = 22663\), 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) \(\{0, \frac{1}{4}, \frac{1}{16}, \frac{1}{64}, \ldots\}\)
   
   (b) \(\{0\} \cup \left\{\frac{n+5}{n} \mid n \in \mathbb{Z^+}\right\}\)
   
   (c) \([0, \infty) \cap 5\mathbb{Z}\)

10. Suppose \(p \geq 83\) is an unknown prime. Find all solutions to \(x^2 + 80 \equiv 18x \mod p\). Note that your solutions will be mod \(p\).

11. Consider the inequality:

   \[8^n < n!\]

   (a) Find the smallest positive integer \(n_0\) for which this is true. Do this however you wish.
   
   (b) Prove by induction that \(8^n < n!\) 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 \((c, a) = \gcd(c, b) = 1\).