1. Given $A = 32219517869$ and $B = 163950325$. \[15 \text{ pts}\]

(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:

\[
\begin{align*}
x & \equiv 5 \mod 17 \\
x & \equiv 8 \mod 12 \\
x & \equiv 3 \mod 5
\end{align*}
\]

3. For each of $n = 58, 436, 8979, 60342$ 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 150 to the linear system: \[10 \text{ pts}\]

\[72x \equiv 114 \mod 150\]

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. \[15 \text{ pts}\]

6. It’s a fact that $r = 7$ is a primitive root mod 11. \[15 \text{ pts}\]

(a) Use this to construct a table of indices for this primitive root.

(b) Use the table of indices to solve the equation: $x^4 \equiv 4 \mod 11$. Your answer(s) should be mod 11.

(c) Use the table of indices to solve the equation: $3^x \equiv 4 \mod 11$. Your answer(s) should be mod 10.

7. Calculate the following Jacobi symbols: \[15 \text{ pts}\]

(a) \[\left(\frac{2272}{1137}\right)\]

(b) \[\left(\frac{2272}{29231}\right)\]
8. Suppose you intercept the following ciphertext from Alice to Bob: 

\[ 7108 \ 2614 \ 15793 \ 12599 \ 16830 \ 17346 \ 7801 \]

You know that Bob’s public key is \((e, n) = (1559, 19043)\). Bob thinks this is secure because he doesn’t believe that his \(n\) can be factored easily. Factor \(n = 19043\), 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) \(\{0, \frac{1}{3}, \frac{1}{10}, \frac{1}{64}, \ldots\}\)
   (b) \(3\mathbb{Z}\)
   (c) \([0, \infty) \cap 4\mathbb{Z}\)

10. Suppose \(p \geq 31\) is an unknown prime. Find all solutions to \(x^2 + 30 \equiv 11x \mod p\). 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 \(\gcd(c, a) = \gcd(c, b) = 1\).