1. Given $A = 107938610$ and $B = 1842375$.\[15 \text{ pts}\]

   (a) Find the prime factorizations of $A$ and $B$ and use them to find $\gcd (A, B)$.\[10 \text{ pts}\]

   (b) Find $\gcd (A, B)$ using the Euclidean Algorithm.\[10 \text{ pts}\]

2. Use the Chinese Remainder Theorem to find the smallest and second smallest nonnegative solutions to the system:\[15 \text{ pts}\]

   $x \equiv 7 \mod 10$
   $x \equiv 2 \mod 21$
   $x \equiv 5 \mod 29$

3. For each of $n = 36, 711, 8371, 37823$ 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\[10 \text{ pts}\]

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

   for each.\[10 \text{ pts}\]

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

   $110x \equiv 10 \mod 135$

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.\[15 \text{ pts}\]

6. It’s a fact that $r = 14$ is a primitive root mod 17.\[15 \text{ pts}\]

   (a) Use this to construct a table of indices for this primitive root.\[10 \text{ pts}\]

   (b) Use the table of indices to solve the equation: $x^2 \equiv 15 \mod 17$. Your answer(s) should be mod 17.\[10 \text{ pts}\]

   (c) Use the table of indices to solve the equation: $15^r \equiv 15 \mod 17$. Your answer(s) should be mod 16.\[10 \text{ pts}\]

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

   (a) $(\frac{2163}{1189})$

   (b) $(\frac{2163}{38657})$
8. Suppose you intercept the following ciphertext from Alice to Bob: [15 pts]

\[ 3998 \ 16812 \ 16061 \ 3690 \ 15095 \ 14441 \ 9311 \ 474 \ 13429 \ 15273 \]

You know that Bob’s public key is \((e, n) = (1679, 19493)\). Bob thinks this is secure because he doesn’t believe that his \(n\) can be factored easily. Factor \(n = 19493\), 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. [15 pts]

(a) \(\{0\} \cup \left\{ \frac{n+5}{n} \mid n \in \mathbb{Z}^+ \right\} \)

(b) \(\{0, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \ldots\} \)

(c) \([0, \infty) \cap 3\mathbb{Z}\)

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 \(\mod p\). [15 pts]

11. Consider the inequality: [15 pts]

\[ 5^n < n! \]

(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 \(p \equiv \pm 3 \mod 8\). [15 pts]

13. Prove that for \(a, b \in \mathbb{Z}\) and \(n \in \mathbb{Z}^+\) that if \(a^n \mid b^n\) then \(a \mid b\). [15 pts]

14. Prove that if \(a, b, c \in \mathbb{Z}\) with \(\gcd(a, b) = 1\) and \(c \mid (a + b)\) then \(\gcd(c, a) = \gcd(c, b) = 1\). [15 pts]