Problem 9.1.

1. Simplify the following congruence classes and decide if they are invertible (multiplicative). If they are, compute their inverse. If they are not, for each $[a]_m$ find a congruence class $[b]_m$ such that $[a]_m[b]_m = [0]_m$ and $0 < b < m$.
   (a) $[13]_{380}$
   (b) $[27]_{9999}$
   (c) $[3^{431}]_{29}$
   (d) $[28899]_{28925}$
2. Solve for x:
   (a) $22x + [63]_{132} = [19]_{132}$
   (b) $(9999)x + [35]_{100} = [56]_{100}$

Problem 9.2.

1. For each of the following RSA parameters, determine if they are valid, and if they are, compute a valid decoding exponent d.
   (a) $p = 29$, $q = 41$, $e = 9$.
   (b) $p = 67$, $q = 97$, $e = 11$.
   (c) $p = 5$, $q = 73$, $e = 127$.
2. For the first valid case that you found, what is the ciphertext corresponding to the plaintext $t = 48$? Check that the decryption gives you back the correct plaintext.
3. For the last valid case that you found, what is the plaintext corresponding to the ciphertext $c = 84$? *Hint: You may use a calculator.*

Problem 9.3.

Consider the map from class:

$$\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

that maps each integer $0 \leq k < mn$ to $\psi(k) = (k \bmod m, k \bmod n)$.

1. Consider the pair $(m, n) = (5, 7)$. Fill the 5×7 table for the map ψ just like we did in class (for other numbers m and n).
2. Find $3^{546458} \bmod 5$.
3. Find $3^{546458} \bmod 7$.
4. Using your table from 9.3.1, find $3^{546458} \bmod 35$.

Problem 9.4.

In this problem we develop an explicit formula for computing $\phi(n)$ for any positive integer n in terms of the prime factorization of n.
Recall that by the Chinese Remainder Theorem, if m and n are coprime, then the function

$$\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

that maps each integer $0 \leq k < mn$ to $\psi(k) = (k \bmod m, k \bmod n)$, is a bijection.

1. Show that if k is coprime to mn, then $k \bmod m$ is comprime to m and $k \bmod n$ is coprime to n.
2. Show that if $0 < a < m$ is coprime to m and $0 < b < n$ is coprime to n, then $\psi^{-1}(a, b)$ is coprime to mn.
3. Conclude that if m and n are coprime, then $\phi(mn) = \phi(m)\,\phi(n)$.
4. Using this result and the fact (seen in class) that $\phi(p^k) = p^k - p^{k-1}$ for any prime p and any positive integer k, prove that for any positive integer n,

   $$\phi(n) = n \prod_p \left(1 - \frac{1}{p}\right)$$

   where the product is over all prime factors of n.
   Hint: write n as a product of prime powers, that is, $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$.

Problem 9.5.

In this problem, we study the computational complexity of the decrypting operation in RSA. Let $m = p \cdot q$ be an RSA modulus where p and q are some large prime numbers. Let e be a valid RSA encoding exponent, and let d be the corresponding decoding exponent. You know d, and you receive a ciphertext c for an unknown plaintext t (i.e., $[c]_m = [t]_m^e$). We are interested in finding a fast way to decrypt c.
In the following, suppose that for any non-negative integers x, y and z with $x < z$ and $y < z$, the exponentiation $x^y \bmod z$ can be computed with $(\log_2 z)^3$ elementary operations.

1. About how many elementary operations are performed by the decryption method given in class? *(Hint: only exponentiations are costly, the rest can be neglected.)*
2. In an attempt to go faster, one can try to perform the decryption modulo p and modulo q, and combine the results with the Chinese Remainders Theorem (instead of decrypting directly modulo m). To do so, we replace the decoding exponent d by the pair of exponents $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$.
   (a) Show that $[c]_p^{d_p} = [t]_p$ and $[c]_q^{d_q} = [t]_q$.
   (b) Describe how to recover $[t]_m$ from $[t]_p$ and $[t]_q$.
   (c) About how many elementary operations are performed by this decryption method? *(Hint: again, only exponentiations are costly, the rest can be neglected.)*
3. How do these two methods compare, assuming that p and q are of the same size (i.e., $\log_2 p \approx \log_2 q$).
