## 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) $[13]_{380}$

   **Solution:**

| $\gcd(a,b)$ | $a = bq + r$ | q | $\tilde{u}$ | $\tilde{v}$ | $u = \tilde{v}$ | $v = \tilde{u} - q\tilde{v}$ |
|---|---|---|---|---|---|---|
| $\gcd(380, 13)$ | $380 = 13 \times 29 + 3$ | 29 | | | -4 | 117 |
| $\gcd(13, 3)$ | $13 = 3 \times 4 + 1$ | 4 | 1 | -4 | 1 | -4 |
| $\gcd(3, 1)$ | $3 = 1 \times 3 + 0$ | 3 | 0 | 1 | 0 | 1 |
| $\gcd(1, 0)$ | $12 = 3 \times 4 + 0$ | 4 | 1 | 0 | | |

   Therefore, $1 = -4 \times 380 + 117 \times 13 \implies [1]_{380} = [117]_{380}[13]_{380}$. Which implies that $[117]_{380}$ is the inverse.

   **Relevant slides : 409 - 416, 417 - 419**

   (b) $[27]_{9999}$

   **Solution:**

   Both 27 and 9999 are divisible by 9 since the sum of their digits is $0 \bmod 9$, so we can deduce that 27 is not invertible mod 9999. Furthermore, 1111 is a number smaller than 9999 and such that $[27]_{9999}[1111]_{9999} = [3]_{9999}[9999]_{9999} = [0]_{9999}$.

   **Relevant slides : 417**

   (c) $[3^{431}]_{29}$

   **Solution:**

   Note that by Euler's theorem $[3^{28}]_{29} = [1]_{29}$.

   Therefore, $[3^{431}]_{29} = [(3^{28})^{15}]_{29}[3^{11}]_{29} = [3^{11}]_{29} = [3^2]_{29}[(3^3)^3]_{29} = [9]_{29}[(-2)^3]_{29} = [-72]_{29} = [-14]_{29} = [15]_{29}$.

   Then, $[3^{431}]$ is invertible and its inverse is $[2]_{29}$, since $[15]_{29}[2]_{29} = [1]_{29}$

   **Relevant slides : 417, 479**

   (d) $[28899]_{28925}$

**Solution:**

We apply the Euclidean algorithm.

| $\gcd(a,b)$ | $a = bq + r$ |
|---|---|
| $\gcd(28925, 28899)$ | $28925 = 28899 \times 1 + 26$ |
| $\gcd(28899, 26)$ | $28899 = 26 \times 1111 + 13$ |
| $\gcd(26, 13)$ | $26 = 13 \times 2 + 0$ |
| $\gcd(13, 0) = 13$ | |

Since $\gcd(28925, 28899) = 13$, 28899 is not invertible mod 28925. By computing $28925/13 = 2225$ we have found the "$b$" that was asked: $[28899]_{28925}[2225]_{28925} = [0]_{28925}$.

**Relevant slides : 409 - 416, 417 - 419**

2. Solve for $x$:

   (a) $22x + [63]_{132} = [19]_{132}$

**Solution:**

We have

$$22x + [63]_{132} = [19]_{132} \iff 22x = [19]_{132} - [63]_{132} = [-44]_{132}$$

Note that $[22]_{132}$ is not invertible. Because $22 = 2 \times 11, 132 = 2 \times 11 \times 6$. Therefore $22x = 0$ is true for $x = [0]_{132}, [6]_{132}, [12]_{132}$. Similarly, $22x = -44$ is true for $x = [-2]_{132}, [4]_{132}, [10]_{132}, ....$

**Relevant slide : 386**

   (b) $(9999)x + [35]_{100} = [56]_{100}$

**Solution:**

As in the previous question we have

$$9999x + [35]_{100} = [56]_{100} \iff 9999x = [21]_{100}. \iff -1x = [21]_{100}$$

$-1$ is invertible in modulo 100. Therefore, there is only a single solution which is $[-21]_{100} = [79]_{100}$.

**Relevant slide : 386**

---

**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) $p = 5$, $q = 73$, $e = 127$.

**Solution:**

All the numbers $p$ and $q$ are prime, which is good.
The encoding exponent $e$ is valid if it is coprime with $k = \text{lcm}(p-1, q-1)$ (the least common multiple).

(a) $k = \text{lcm}(p-1, q-1) = \text{lcm}(28, 40) = \text{lcm}(2^2 \times 7, 2^3 \times 5) = 2^3 \times 5 \times 7 = 280$. The encoding exponent $e$ is coprime with $k$ so it is valid. To find the decoding exponent, we apply the extended Euclidean algorithm and find that $1 = \gcd(280, 9) = 280 \cdot 1 + 9 \cdot (-31)$, so $d = -31$. Instead of this we can as well use $d' = d + k = -31 + 280 = 249$ as the decoding exponent.

| $\gcd(a, b)$ | $a = bq + r$ | $u = \tilde{v}$ | $v = (\tilde{u} - q\tilde{v})$ |
|---|---|---|---|
| $\gcd(280, 9)$ | $280 = 9 \times 31 + 1$ | 1 | $0 - 31 \times (1) = -31$ |
| $\gcd(9, 1)$ | $9 = 1 \times 9 + 0$ | 0 | 1 |
| $\gcd(1, 0)$ | | 1 | 0 |

(b) $k = \text{lcm}(p-1, q-1) = \text{lcm}(66, 96) = \text{lcm}(2 \times 3 \times 11, 2^5 \times 3) = 2^5 \times 3 \times 11$. The encoding exponent $e = 11$ is not coprime with $k$ so it is not valid.

(c) $k = \text{lcm}(p-1, q-1) = \text{lcm}(4, 72) = \text{lcm}(2^2, 2^3 \times 3^2) = 2^3 \times 3^2 = 72$. The encoding exponent $e = 127$ is prime, and is coprime with 72, so it is valid. The decoding exponent is obtained using the extended Euclidean algorithm: $1 = \gcd(127, 72) = -127 \cdot 17 + 72 \cdot 30$, so $d = -17$. Note that the Bézout equality ($1 = ed + kl$) holds as well when replacing $d$ with $d + k$ (and $l$ with $l - e$). So we can use $d + k = 55$ as the decoding exponent.

| $\gcd(a, b)$ | $a = bq + r$ | $u = \tilde{v}$ | $v = (\tilde{u} - q\tilde{v})$ |
|---|---|---|---|
| $\gcd(127, 72)$ | $127 = 72 \times 1 + 55$ | $-17$ | $13 + 1 \times 17 = 30$ |
| $\gcd(72, 55)$ | $72 = 55 \times 1 + 17$ | 13 | $-4 - 1 \times 13 = -17$ |
| $\gcd(55, 17)$ | $55 = 17 \times 3 + 4$ | $-4$ | $1 - 3 \times (-4) = 13$ |
| $\gcd(17, 4)$ | $17 = 4 \times 4 + 1$ | 1 | $0 - 4 \times 1 = -4$ |
| $\gcd(4, 1)$ | $4 = 1 \times 4 + 0$ | 0 | $1 - 4 \times 0 = 1$ |
| $\gcd(1, 0) = 1$ | | 1 | 0 |

**Relevant slides : 527 - 534**

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.

**Solution:**

$[c]_{29*41} = ([48]_{29*41})^9 = [997]_{29*41}$. The decoding exponent is 249, and as expected we find $([997]_{29*41})^{249} = [48]_{29*41} = [t]_{29*41}$.

**Relevant slides : 527 - 534**

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.*

**Solution:**

$[t]_{365} = ([c]_{365})^{55} = [224]_{365}$.

**Relevant slides : 527 - 534**

---

## 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 $5 \times 7$ table for the map $\psi$ just like we did in class (for other numbers $m$ and $n$).

   **Solution:**

   The table is

   | | $[0]_7$ | $[1]_7$ | $[2]_7$ | $[3]_7$ | $[4]_7$ | $[5]_7$ | $[6]_7$ |
   |---|---|---|---|---|---|---|---|
   | $[0]_5$ | $[0]_{35}$ | $[15]_{35}$ | $[30]_{35}$ | $[10]_{35}$ | $[25]_{35}$ | $[5]_{35}$ | $[20]_{35}$ |
   | $[1]_5$ | $[21]_{35}$ | $[1]_{35}$ | $[16]_{35}$ | $[31]_{35}$ | $[11]_{35}$ | $[26]_{35}$ | $[6]_{35}$ |
   | $[2]_5$ | $[7]_{35}$ | $[22]_{35}$ | $[2]_{35}$ | $[17]_{35}$ | $[32]_{35}$ | $[12]_{35}$ | $[27]_{35}$ |
   | $[3]_5$ | $[28]_{35}$ | $[8]_{35}$ | $[23]_{35}$ | $[3]_{35}$ | $[18]_{35}$ | $[33]_{35}$ | $[13]_{35}$ |
   | $[4]_5$ | $[14]_{35}$ | $[29]_{35}$ | $[9]_{35}$ | $[24]_{35}$ | $[4]_{35}$ | $[19]_{35}$ | $[34]_{35}$ |

2. Find $3^{546458} \bmod 5$.

   **Solution:**

   $3^{546458} \bmod 5 \equiv (3^2)^{273229} \bmod 5 \equiv (-1)^{273229} \bmod 5 \equiv -1 \bmod 5 \equiv 4 \bmod 5$.

3. Find $3^{546458} \bmod 7$.

   **Solution:**

   $3^{546458} \bmod 7 \equiv 3^2 \cdot (3^3)^{182152} \bmod 7 \equiv 9 \cdot (-1)^{182152} \bmod 7 \equiv 9 \equiv 2 \bmod 7$.

4. Using your table from 9.3.1, find $3^{546458} \bmod 35$.

   **Solution:**

   Read from the table that $\psi^{-1}(3^{546458} \bmod 5, 3^{546458} \bmod 7) = \psi^{-1}(4 \bmod 5, 2 \bmod 7) = (9 \bmod 35)$.

---

## 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 $n$.

   **Solution:**

   Since $k$ is coprime to $mn$, then $k$ has no prime factors in common with $m$ and $n$. Let $a = k \bmod m$. Then $a = bm + k$. Any prime factor of $m$ divides $bm$ but not $k$, therefore it does not divide $a$, which means that $a$ is coprime to $m$.
   The same reasoning applies to $b = k \bmod n$.

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 $mn$.

   **Solution:**

   From the definition of $\psi$ and the fact that it is bijective, one has that for any $(a, b)$ there is a unique $k = \psi^{-1}(a, b)$ with $0 < k < mn$ such that $a = k \bmod m$ and $b = k \bmod n$. Hence, we can write $k = bm + a$. Since $a$ is coprime to $m$, any factor of $m$ divides $bm$ but not $a$, therefore $k$ has no common factors with $m$. Applying the same reasoning to $b$ shows that $k$ also has no common factors with $n$, therefore $k$ has no common factors with $mn$, that is, $k$ is coprime to $mn$.

3. Conclude that if $m$ and $n$ are coprime, then $\phi(mn) = \phi(m)\,\phi(n)$.

   **Solution:**

   We showed in the previous two points that there is a bijection between the positive integers less than $mn$ that are coprime to $mn$ and the pairs $(a, b)$ where $a$ is a positive integer less than $m$ and coprime to $m$, and $b$ is a positive integer less than $n$ and coprime to $n$. Therefore, these two sets have the same cardinality. Also, the number of positive integers less than $mn$ that are coprime to $mn$ is precisely $\phi(mn)$, and the number of pairs $(a, b)$ where $a$ is a positive integer less than $m$ and coprime to $m$, and $b$ is a positive integer less than $n$ and coprime to $n$ is $\phi(m) \cdot \phi(n)$. Hence, $\phi(mn) = \phi(m)\,\phi(n)$.

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, $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$.*

**Solution:**

Following the hint, let $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$. Any two prime powers are coprime, therefore we can apply the result of point 3 recursively to get

$$\begin{aligned}\phi(n) &= \phi(p_1^{k_1})\,\phi(p_2^{k_2}) \cdots \phi(p_m^{k_m}) \\ &= \prod_i \phi(p_i^{k_i}).\end{aligned}$$

Next, using the fact that $\phi(p^k) = p^k - p^{k-1}$ for any prime power $p^k$, we can write

$$\begin{aligned}\phi(n) &= \prod_i (p_i^{k_i} - p_i^{k_i - 1}) \\ &= \prod_i p_i^{k_i} \left(1 - \frac{1}{p_i}\right) \\ &= \left[\prod_i p_i^{k_i}\right] \left[\prod_i \left(1 - \frac{1}{p_i}\right)\right] \\ &= n \prod_i \left(1 - \frac{1}{p_i}\right)\end{aligned}$$

which is what we wanted to prove.

---

**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.)*

   **Solution:**

   The decryption consists in computing the exponentiation $c^d \bmod m$. It takes approximately $(\log_2 m)^3$ elementary operations.

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 $[c]_q^{d_q} = [t]_q$.

**Solution:**

Since $d_p = d \bmod (p-1)$ we can write $d = (p-1)k + d_p$ for some integer $k$. We compute $[c]_p^{d_p}$ and obtain:

$$[c]_p^{d_p} = [c^{d_p}]_p = [c^{d-(p-1)k}]_p = [c^d]_p [c^{-(p-1)k}]_p = [c^d]_p \,,$$

where the last equality uses Fermat's theorem.
RSA says that $[c^d]_{pq} = [t]_{pq}$. With the Chinese Remainders Theorem we get the same but with modulus $p$ instead of $pq$, i.e., $[c^d]_p = [t]_p$.
Putting everything together, we obtain that $[c]_p^{d_p} = [c^d]_p = [t]_p$.
We prove the second equality in a similar way.

(b) Describe how to recover $[t]_m$ from $[t]_p$ and $[t]_q$.

**Solution:**

We use the method seen in class to invert the map of the Chinese Remainders Theorem. Let $t_p = t \bmod p$ and $t_q = t \bmod q$. First, we use the extended Euclidean algorithm to find integers $u$ and $v$ such that $pu + qv = 1$. Then,

$$t = qvt_p + put_q \bmod m.$$

(c) About how many elementary operations are performed by this decryption method? *(Hint: again, only exponentiations are costly, the rest can be neglected.)*

**Solution:**

With this method, two exponentiations are performed: $c_p^{d_p} \bmod p$ and $c_q^{d_q} \bmod q$. This requires a total of $(\log_2 p)^3 + (\log_2 q)^3$ elementary operations.

3. How do these two methods compare, assuming that $p$ and $q$ are of the same size (i.e., $\log_2 p \approx \log_2 q$).

**Solution:**

The first method costs $(\log_2 m)^3$ elementary operations. For the second method, observe that $\log_2 p \approx \log_2 q \approx \frac{\log_2 m}{2}$. So the number of elementary operations is

$$(\log_2 p)^3 + (\log_2 q)^3 \approx \frac{(\log_2 m)^3}{2^3} + \frac{(\log_2 m)^3}{2^3} = \frac{1}{4}(\log_2 m)^3.$$

It is approximately four times faster.