Problem 1.

a. Solving the congruence \( 72x \equiv 36 \pmod{376} \) is equivalent to solving the equation \( 72x + 376y = 36 \). Now, using Euclid’s algorithm, we compute \((72, 376) = 8 \). Since 8 does not divide 36, the equation \( 72x + 376y = 36 \) (and hence the congruence) has no solutions in integers.

b. The problem is to find a common solution to the system of three congruences:

\[
\begin{align*}
  x &\equiv 1 \pmod{9} , \\
  x &\equiv 3 \pmod{7} , \\
  x &\equiv 4 \pmod{5} .
\end{align*}
\]

To do this we use the Chinese Remainder Theorem as follows. First, we solve the first two congruences: it follows from (1) and (2) that \( x = 1+9k = 3+7m \) for some \( m, k \in \mathbb{Z} \). This gives \( 9k - 7m = 2 \); whence \( m = k = 1 \) and \( x = 10 \). Thus, by the Chinese Remainder Theorem, a common solution of (1) and (2) is given by

\[ x \equiv 10 \pmod{63} . \]  

(4)

Now, we find a common solution to the system of congruences (3) and (4). We have \( x = 4 + 5s = 10 + 63t \), so that \( 5s - 63t = 6 \). Since \( 5 \cdot (-25) + 63 \cdot 2 = 1 \), we see that \( s = -150, t = -12 \) and \( x = -746 \). Thus, the smallest positive integer in this last set corresponds to \( k = 3 \) and is equal to \( 315 \cdot 3 - 746 = 945 - 746 = 199 \).

Problem 2.

a. This is a standard application of the Fundamental Theorem of Arithmetic. Write \( a, b \) and \( c \) as products of primes: \( a = \prod_{i=1}^{n} p_i^{e_i}, \ b = \prod_{i=1}^{n} p_i^{f_i} \) and \( c = \prod_{i=1}^{n} p_i^{s_i} \). Now, observe that \( (a, b) = 1 \) implies that either \( e_i \) or \( f_i \) is 0 for each \( i = 1, 2, 3, \ldots, n \). Hence the sum \( e_i + f_i \) is either equal to \( e_i \) or \( f_i \), and \( \min(e_i + f_i, s_i) \) is either \( \min(e_i, s_i) \) or \( \min(f_i, s_i) \). It follows that
contradiction proves the result.

in each and∈ of Arithmetic, we can write\(c\) for all \(i = 1, 2, \ldots, n\), which is equivalent to the equation \((ab, c) = (a, c)(b, c)\).

b. Assume to the contrary that there is an integer \(c_0 \in \mathbb{Z}\), such that we have \((a + bx, c_0) \neq 1\) for any \(x \in \mathbb{Z}\). By the Fundamental Theorem of Arithmetic, we can write \(c_0 = p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}\), where \(p_i\)'s are some primes and \(e_i > 0\) for all \(i = 1, 2, \ldots, n\). Now, for each \(i\), define the sets

\[Z_i := \{ x \in \mathbb{Z} : p_i \mid (a + xb) \} \subseteq \mathbb{Z}.\]

Clearly, if \((a + bx, c_0) \neq 1\) for all \(x \in \mathbb{Z}\), then for each \(x \in \mathbb{Z}\) there is \(i = 1, 2, \ldots, n\), such that \(p_i\) divides \(a + bx\). Hence, we have

\[\mathbb{Z} = \bigcup_{i=1}^{n} Z_i,\]

and in particular, \(Z_i \neq \emptyset\) for some \(i\)'s. Note, if \(Z_i \neq \emptyset\), then \(p_i\) does not divide \(b\) (for otherwise \(p_i \mid b\) and \(p_i \mid (a + bx)\) would imply that \(p_i \mid a\) and we would get \(p_i \mid (a, b)\) with contradiction to the fact that \((a, b) = 1\). Thus, we have \((b, p_i) = 1\) whenever \(Z_i \neq \emptyset\), and hence in this case \(br_i \equiv 1\) (mod \(p_i\)) for some \(r_i \in \mathbb{Z}\) by Bezout’s identity. Now, if \(x \in Z_i\), we have \(bx \equiv -a\) (mod \(p_i\)) and hence \(x \equiv -ar_i + 1\) (mod \(p_i\)).

Summing up, \((5)\) says that every integer \(x\) is congruent to one of the numbers \(-ar_i + 1\) (modulo \(p_i\)), where \(r_i\) depends only on \(b\) and \(p_i\) (and not on \(x\)). This obviously contradicts the Chinese Remainder Theorem: indeed, by the latter theorem, we can always find \(x \in \mathbb{Z}\) such that \(x \equiv -ar_i + 1\) (mod \(p_i\)) for each \(i = 1, 2, \ldots, n\), but such \(x\) can’t be in any of the sets \(Z_i\)'s. This contradiction proves the result.

**Problem 3.**

a. If \(f\) is injective then \(|f(X)| = |X|\). Since \(|X| = |Y|\), this implies \(|f(X)| = |Y|\). But \(f(X) \subseteq Y\). Hence \(f(X) = Y\), which means that \(f\) is surjective. Conversely, if \(f\) is surjective then \(|X| \geq |f(X)| = |Y|\). This implies that \(|X| = |f(X)|\), because \(|X| = |Y|\), and therefore \(f\) is injective.

b. The main problem is to compute the values of \(\sigma\). First of all, we obviously have \(\sigma(0) = 0\), \(\sigma(1) = 1\) and \(\sigma(10) = 7\). The latter is true because \(10 \equiv -1\) (mod \(11\)) and hence \(4 \cdot 10^2 - 3 \cdot 10^7 \equiv 4 \cdot (-1)^2 - 3 \cdot (-1)^7 = 4 + 3 = 7\). For other values of \(n\), we can also do arithmetic modulo 11 to simplify calculations. For example, take \(n = 7\). We have \(7^2 = 49 \equiv 5 \Rightarrow\)
\[7^3 \equiv 35 \equiv 2 \Rightarrow 7^4 \equiv 14 \equiv 3 \Rightarrow 7^5 \equiv 21 \equiv -1 \Rightarrow 7^6 \equiv -7 \equiv 4 \Rightarrow 7^7 \equiv 28 \equiv 6. \text{ Thus, } 4 \cdot 7^2 - 3 \cdot 7^7 \equiv 4 \cdot 5 - 3 \cdot 6 = 20 - 18 = 2, \text{ so we get } \sigma(7) = 2.\]

As a result, we obtain the permutation

\[
\sigma = \left( \begin{array}{cccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
1 & 2 & 7 & 10 & 6 & 4 & 11 & 3 & 9 & 5 & 8 
\end{array} \right) \quad (6)
\]

(Note that we have shifted all the numbers by 1 because permutations act on the indices numbering the position of elements in a finite set.) The complete factorization of our permutation is given by

\[
\sigma = (1) (2) (3,7,11,8) (4,10,5,6)(9). \quad (7)
\]

A factorization into a product of transpositions is

\[
\sigma = (1,2)(1,2)(2,1)(2,1)(3,8)(3,11)(3,7)(4,6)(4,5)(4,10)(9,10)(9,10).
\]

Finally, we see from (7) that \(\text{sign}(\sigma) = 1 \cdot 1 \cdot (-1) \cdot (-1) \cdot 1 = 1.\) Thus \(\sigma\) is an even permutation. (Here we use the fact that an \(r\)-cycle is an even permutation iff \(r\) is odd, see HW problem 2.26.)

**Problem 4.**

\[a.\] See (the proof of) Proposition 2.55(ii) on page 137.

\[b.\] Define a function \(\varepsilon: \{1, 2, \ldots, r\} \to \{0, 1\}\) by the rule: \(\varepsilon(l) = 1\) if \(k_l = 0\), and \(\varepsilon(l) = l\) if \(k_l \neq 0\). Since the order of a cycle of length \(l\) is equal to \(l\), by part (a), we have

\[
|\sigma| = \text{lcm}\{\varepsilon(1), \varepsilon(2), \ldots, \varepsilon(r)\}.
\]