Problem 1.

a) The multiplicative inverse of 7 modulo 11 exists (and is equal to 8). The multiplicative inverse of 6 modulo 8 doesn’t exist. The multiplicative inverse of 5 modulo 8 exists (and is equal to 5).

b) Let $x$ be the multiplicative inverse of $a$ modulo $b$. That is, $ax \equiv 1 \pmod{b}$ or equivalently,

$$ax = bk + 1 \quad \text{for some integer } k$$

which is equivalent to

$$ax - bk = 1.$$ 

Take $y := -k$ and recall that Bézout Lemma states that every integer of the form $ax + by$ is a multiple of the greatest common divisor of $a$ and $b$, $d := \gcd(a, b)$. Consequently, we can find an integer $x$ such that $ax \equiv 1 \pmod{b}$ if and only if $\gcd(a, b) = 1$.

Swapping the roles of $a$ and $b$ we can conclude that $\gcd(a, b) = 1$ is also a necessary and sufficient condition for existence of the multiplicative inverse of $b$ modulo $a$.

For the previous examples we can check that

- $\gcd(7, 11) = 1$ hence the multiplicative inverse of 7 modulo 11 exists.
- $\gcd(6, 8) = 2 \neq 1$ hence the multiplicative inverse of 6 modulo 8 doesn’t exist.
- $\gcd(5, 8) = 1$ hence the multiplicative inverse of 5 modulo 8 exists.

c) Recall the Euclid Algorithm to find the greatest common divisor of two numbers $a$ and $b$. At each step $k = 0, 1, \ldots$, the algorithm finds the quotient $q_k$ and remainder $r_k$ such that

$$r_{k-2} = q_k r_{k-1} + r_k,$$

starting with $r_{-2} := a$ and $r_{-1} := b$. In other words, the algorithm produces a sequence of quotients and reminders as:

\begin{align*}
  a &= q_0 b + r_0 & \text{(at step } k = 0) \\
  b &= q_1 r_0 + r_1 & \text{(at step } k = 1) \\
  r_0 &= q_2 r_1 + r_2 & \text{(at step } k = 2) \\
  r_1 &= q_3 r_2 + r_3 & \text{(at step } k = 3) \\
  & \vdots \\
  r_{N-3} &= q_{N-2} r_{N-4} + r_{N-2} & \text{(at step } k = N-1) \\
  r_{N-2} &= q_N d + r_N & \text{(at step } k = N) 
\end{align*}

and terminates at some step $N$ when $r_N = 0$. The last non-zero remainder is $d := \gcd(a, b)$. That is,

\begin{align*}
  r_{N-3} &= q_{N-2} r_{N-4} + d & \text{(at step } k = N-1) \\
  r_{N-2} &= q_N d + 0 & \text{(at step } k = N) 
\end{align*}
Rewriting the equation of step \( N - 1 \), we have

\[ d = r_{N-3} - q_{N-1}r_{N-2}. \]

Now, we can use the equation for step \( N - 2 \) to write \( r_{N-2} = r_{N-4} - q_{N-2}r_{N-3} \) and replace this in the above equation to get:

\[ d = (1 + q_{N-1}q_{N-2})r_{N-3} - q_{N-1}r_{N-4} \]

We can again use the equation for step \( N - 3 \) and write \( r_{N-3} = r_{N-5} - q_{N-3}r_{N-4} \) and replace \( r_{N-3} \) in the above equation to get:

\[ d = (1 + q_{N-1}q_{N-2})r_{N-5} - (q_{N-3} + q_{N-1}q_{N-2} + q_{N-1})r_{N-4} \]

Continuing this procedure up to very first step \( k = 0 \), we will be able to write \( d \) as a linear combination of \( r_{-2} = a \) and \( r_{-1} = b \):

\[ d = sa - tb \]

Now, if \( d = \gcd(a, b) = 1 \), we have found numbers \( s \) and \( t \) such that

\[ sa = 1 + bt \]

which means \( s \) is the multiplicative inverse of \( a \) modulo \( b \): \( sa \equiv 1 \pmod{b} \).

d)  i. Running the Euclid algorithm on the pair of integers 148 and 57 we have

\[
\begin{align*}
148 &= 2 \times 57 + 34, \\
57 &= 1 \times 34 + 23, \\
34 &= 1 \times 23 + 11, \\
23 &= 2 \times 11 + 1, \\
\end{align*}
\]

(note that we have not written down the very last trivial step). Hence, starting from the last equation and going back to top, we will have

\[
\begin{align*}
1 &= 23 - 2 \times 11 \\
&= 23 - 2 \times (34 - 1 \times 23) \\
&= 3 \times 23 - 2 \times 34 \\
&= 3 \times (57 - 1 \times 34) - 2 \times 34 \\
&= 3 \times 57 - 5 \times 34 \\
&= 3 \times 57 - 5 \times (148 - 2 \times 57) \\
&= 13 \times 57 - 5 \times 148 \\
\end{align*}
\]

which shows \( 13 \times 57 \equiv 1 \pmod{148} \).

ii. Running the Euclid algorithm on the pair of integers 341 and 123 we have

\[
\begin{align*}
341 &= 2 \times 123 + 95, \\
123 &= 1 \times 95 + 28, \\
95 &= 3 \times 28 + 11, \\
28 &= 2 \times 11 + 6, \\
11 &= 1 \times 6 + 5, \\
6 &= 1 \times 5 + 1. \\
\end{align*}
\]
Thus,

\[ 1 = 6 - 1 \times 5 \]
\[ = 6 - 1 \times (11 - 1 \times 6) \]
\[ = 2 \times 6 - 1 \times 11 \]
\[ = 2 \times (28 - 2 \times 11) - 1 \times 11 \]
\[ = 2 \times 28 - 5 \times 11 \]
\[ = 2 \times 28 - 5 \times (95 - 3 \times 28) \]
\[ = 17 \times 28 - 5 \times 95 \]
\[ = 17 \times (123 - 95) - 5 \times 95 \]
\[ = 17 \times 123 - 22 \times 95 \]
\[ = 17 \times 123 - 22 \times (341 - 2 \times 123) \]
\[ = 61 \times 123 - 22 \times 341 \]

which shows \( 61 \times 123 \equiv 1 \pmod{341} \).

iii. Running the Euclid algorithm on the pair of integers 921 and 257 we have

\[
\begin{align*}
921 &= 3 \times 257 + 150, \\
257 &= 1 \times 150 + 107, \\
150 &= 1 \times 107 + 43, \\
107 &= 2 \times 43 + 21, \\
43 &= 2 \times 21 + 1.
\end{align*}
\]

Therefore,

\[
1 = 43 - 2 \times 21
\]
\[
= 43 - 2 \times (107 - 2 \times 43)
\]
\[
= 5 \times 43 - 2 \times 107
\]
\[
= 5 \times (150 - 1 \times 107) - 2 \times 107
\]
\[
= 5 \times 150 - 7 \times 107
\]
\[
= 5 \times 150 - 7 \times (257 - 1 \times 150)
\]
\[
= 12 \times 150 - 7 \times 257
\]
\[
= 12 \times (921 - 3 \times 257) - 7 \times 257
\]
\[
= 12 \times 921 - 43 \times 257
\]

Hence, \( -43 \times 257 \equiv 1 \pmod{921} \) which means the multiplicative inverse of 257 is \( -43 \equiv 878 \pmod{921} \).

Problem 2.

a) The cardinality of \( \mathcal{A}_n \) and the number of terms on the left hand side of (1) is \((n + 1)^n\). By the uniqueness of the factorization, for each element \( m \) of \( \mathcal{A}_n \), the term \( 1/m \) appears in the expansion of the product on the left. Thus, the expansion of this product is a rearrangement of the finite sum on the right.

b) Recall that for any \( a \neq 1 \),

\[
\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.
\]
Hence,

\[
1 + \frac{1}{p_j} + \ldots + \frac{1}{p_j^{m}} = \sum_{i=0}^{n} \frac{1}{p_j^i} = \frac{1 - \frac{1}{p_j^{n+1}}}{1 - \frac{1}{p_j}} = \frac{1}{p_j - 1} = 1 + \frac{1}{p_j - 1}
\]

e) Using (1), we obtain that \(\ln \sum_{m \in \mathcal{A}_n} \frac{1}{m} = \ln \prod_{i=1}^{n} \frac{1}{p_i} \). Since \(\ln(\cdot)\) is a monotonous function, using point b), we have that

\[
\ln \prod_{i=1}^{n} \left(1 + \frac{1}{p_i - 1}\right) = \sum_{i=1}^{n} \ln \left(1 + \frac{1}{p_i - 1}\right).
\]

We can check that for \(x \geq 0\), \(\ln(1 + x) \leq x\). As a result,

\[
\sum_{i=1}^{n} \ln \left(1 + \frac{1}{p_i - 1}\right) \leq \sum_{i=1}^{n} \frac{1}{p_i - 1}
\]

Putting all these results together, we obtain \(\sum_{i=1}^{n} \frac{1}{p_i - 1} \geq \ln \sum_{m \in \mathcal{A}_n} \frac{1}{m}\).

d) \(\{1, \ldots, n\} \subseteq \mathcal{A}_n\) because for all \(j \in \{1, \ldots, n\}\), the unique factorization of \(j\) contains only primes from \(\{p_1, \ldots, p_n\}\) as \(p_n \geq n\). Also the multiplicity of each prime needs to be at most \(n\), since \(p_n^{n+1} \geq 2^{n+1} > n\).

This proves that

\[
\ln \sum_{m \in \mathcal{A}_n} \frac{1}{m} \geq \ln \sum_{m=1}^{n} \frac{1}{m}.
\]

As concerns the left hand side, note that for \(j \geq 2\),

\[
\frac{1}{p_j - 1} < \frac{1}{p_j - 1}.
\]

In addition, if \(j = 1\), then

\[
\frac{1}{p_1 - 1} = \frac{1}{2 - 1} = 1.
\]

Hence \(\sum_{j=1}^{n} \frac{1}{p_j - 1} \leq 1 + \sum_{j=2}^{n} \frac{1}{p_j - 1} = 1 + \sum_{j=1}^{n-1} \frac{1}{p_j}\).

e) We already know that \(\sum_{j=1}^{n} \frac{1}{j} \geq \ln(n) \geq \ln(n - 1)\) Hence using the upper-bound of (2),

\[
\sum_{j=1}^{n-1} \frac{1}{p_j} \geq \ln(\ln(n - 1)) - 1
\]

which shows \(\sum_{j=1}^{n} \frac{1}{p_j} = \Omega(\log \log n)\).

\textbf{Problem 3.}

\(^1\text{Define } f(x) = \ln(x+1) \text{ and } g(x) = x. \text{ Then } g(0) = f(0) = 0 \text{ and } g'(x) = 1 > \frac{1}{1+x} = f'(x) \text{ for any } x \geq 0. \text{ Consequently } f(x) \leq g(x) \text{ for any } x \geq 0.\)
a) **Base Step:** The claim clearly holds for \( n = 1, 2^2 - 1 = 3 \mid 3 \).

**Induction Step:** Assume \( 2^{2n} - 1 \mid 3 \). That is \( 2^{2n} = 3k + 1 \) for some integer \( k \). Then
\[
2^{2(n+1)} - 1 = 2^{2n} \times 4 - 1 = 12k + 4 - 1 = 12k + 3 \mid 3.
\]

b) **Base Step:** The claim clearly holds for \( n = 1, (a - b) \mid (a - b) \).

**Induction Step:** Assume \( (a^n - b^n) \mid (a - b) \). We can always write
\[
a^{n+1} - b^{n+1} = a^{n+1} - a^n b + a^n b - b^n = a^n (a - b) + (a^n - b^n) b \mid (a - b)
\]
because of the assumption \( (a^n - b^n) \mid (a - b) \) (and also the base case \( (a - b) \mid (a - b) \)).

---

**Problem 4.**

**Base Step:** Any shape in \( C_1 \) is clearly *cool*. No matter which square is missing, any shape in \( C_1 \) can be tiled using a single L-shaped tile:

![L-shaped tile](image)

**Induction Step:** Assume that any shape in \( C_n \) is *cool*. In other words, we can tile a \( 2^n \times 2^n \) grid using L-shaped tiles leaving one empty \( 1 \times 1 \) square no matter which square is missing. We shall show that any shape in \( C_{n+1} \) is *cool*, namely, that we can tile a \( 2^{n+1} \times 2^{n+1} \) grid using L-shaped tiles leaving one empty \( 1 \times 1 \) square no matter which square is missing. The \( 2^{n+1} \times 2^{n+1} \) grid consists of four \( 2^n \times 2^n \) grids placed side by side. The square that we want to be empty is hence in one of these four \( 2^n \times 2^n \) sub-grids. Assume without loss of generality this is the bottom right grid:

![Grid](image)

By the induction assumption, we can tile this sub-grid leaving the desired square empty:

![Sub-grid](image)

Furthermore, again using the induction assumption, we can tile each of the three remaining \( 2^n \times 2^n \) grids using L-shaped tiles leaving the closest square to the center empty:
This leaves us with a single L-shaped untiled area in the center which can be tiled using an additional L-shaped tile:

![Diagram showing the single L-shaped untiled area]

Hence, any shape in \( C_{n+1} \) is cool. \( \square \)

**Problem 5.** Suppose \( n = 35 \) and we are proving the claim for \( n + 1 = 36 \). 36 is not prime but \( 36 = 3 \times 12 \). By the induction hypothesis 12 has a prime factorization \( 12 = p_1p_2p_3 \) and 3 is prime hence \( 36 = 3p_1p_2p_3 \). However, \( 36 = 4 \times 9 \) as well and by the induction hypothesis we again have \( 4 = q_1q_2 \) and \( 9 = r_1r_2 \), thus \( 36 = q_1q_2r_1r_2 \) as well. The question is how we know that \( 3, p_1, p_2, \) and \( p_3 \) are the same prime numbers as \( q_1, q_2, r_1, \) and \( r_2 \) (up to a permutation)? They indeed are, but this does not follow from the induction hypothesis. This is called a **breakdown error**. If we try to show that something is unique and we break it down (as we broke down \( n + 1 = rs \)) we need to argue that nothing changes if we break it down a different way (i.e. \( n + 1 = tu \)).