You may use the following consequence of Euclid’s algorithm. Mention it if and when you do so.

**Fundamental Theorem.** If \( a \) and \( b \) are natural numbers, then there are integers \( x \) and \( y \) that solve the equation:

\[
ax + by = \gcd(a, b)
\]
1. Give precise definitions of each of the following (4 points each)

(a) The greatest common divisor of natural numbers $a$ and $b$

The greatest common divisor of $a$ and $b$ is the largest integer $d$ with the property that $d|a$ and $d|b$.

(b) A group $(G, \cdot)$

This is a set with a binary operation satisfying the following:

(i) Associativity. For all $a, b, c \in G$, $(ab)c = a(bc)$.

(ii) Unit. There is an $e \in G$ such that $ae = ea = a$ for all $a \in G$.

(iii) Inverses. For all $a \in G$, there is a $b \in G$ such that $ab = ba = e$.

(c) The order of an element $g \in G$ of a group

The order of $g$, denoted $o(g)$, is the smallest positive integer $n$ such that $g^n = e$, or, if there is no such $n$, then the order of $g$ is infinity.

(d) The group $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ for a given natural number $n > 1$

This is the group of integers (mod $n$) that are relatively prime to $n$, with multiplication (mod $n$) as the binary operation.

(e) The Euler $\phi$ function $\phi(n)$

This is the order of the group in (d), or, equivalently, the number of integers between 0 and $n$ that are relatively prime to $n$. 
2. Suppose $a, b$ are natural numbers that satisfy the equation:

$$24a - 23b = 1$$

(a) (5 points) Explain carefully why $a$ and $b$ are relatively prime.

Suppose $d | a$ and $d | b$. Then $d | (24a - 23b)$. In other words, every common divisor of $a$ and $b$ divides 1, so the greatest common divisor divides 1. Thus the greatest common divisor of $a$ and $b$ is 1.

Now let $a = 139$ and $b = 145$ (these satisfy the equation!)

(b) (5 points) Find a natural number $n \leq 138$ such that:

$$n = b^{-1} \text{ in the group } (\mathbb{Z}/139\mathbb{Z})^\times$$

It is immediate from the equation:

$$24 \cdot 139 - (23)(145) = 1$$

that $b^{-1} \equiv -23 \pmod{139}$. But this is not a natural number. To get a natural number, just add 139. This gives:

$$-23 + 139 = 116$$

(c) (10 points) Find an integer $k$ with the property that:

$$k \equiv 2 \pmod{139} \text{ and } k \equiv 3 \pmod{145}$$

“Going backwards” in the Chinese Remainder Theorem gives us an answer of:

$$axt + bys$$

when we seek a number that is congruent to $s \pmod{a}$ and $t \pmod{b}$. In this case, that is:

$$(139)(24)(3) + (145)(-23)(2) = 3338$$
3. (20 points)

(a) (10 points) Suppose $a, b, n$ are natural numbers such that:
\[ \gcd(a, b) = 1, \ a|n \text{ and } b|n \]
Prove that $ab|n$.

Here we must use the Fundamental Theorem:
\[ ax + by = 1 \]
from the first page of the exam. Suppose $a|n$ and $b|n$. Then:
\[ n = axn + byn \]
(multiplying the previous equation by $n$). But $ab|(axn)$ because $b|n$ and $ab|(byn)$ because $a|n$, so:
\[ ab|n \text{ because } n = axn + byn \]

(b) (10 points) Carefully state the Chinese Remainder Theorem, and explain how (a) is used to prove it.

The Chinese Remainder Theorem says that if $\gcd(a, b) = 1$, then:
\[ \mathbb{Z}/ab\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \]
is a bijection, from which it follows that the map on the multiplicative groups is also a bijection.

Since both sets have $ab$ elements, if suffices to prove that the map is an injection. That is, it suffices to show that:
\[ x \equiv y \pmod{a} \text{ and } x \equiv y \pmod{b} \text{ imply that } x \equiv y \pmod{ab} \]
In other words, if $a|(y - x)$ and $b|(y - x)$, we need to know that $ab|(y - x)$. But this is precisely what we just proved in (a).
4. (a) (5 points) Compute the following values of the Euler \( \phi \) function:

\[
\phi(15) = 8 \quad \phi(16) = 8 \quad \phi(36) = 12 \quad \phi(37) = 36 \quad \phi(91) = 72
\]

(b) (15 points) Fill out the following table, listing all the elements \( a \in (\mathbb{Z}/15\mathbb{Z})^\times \), their inverses, and their orders.

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a^{-1} )</th>
<th>( o(a) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>2</td>
</tr>
</tbody>
</table>
5. (a) (5 points) Carefully state Lagrange’s Theorem.

If $G$ is a finite group and $g \in G$, then $o(g) || |G|$.

(b) (5 points) Carefully state Fermat’s Little Theorem.

If $p$ is a prime and $p$ does not divide $a$, then:

$$a^{p-1} \equiv 1 \pmod{p}$$

(c) (5 points) Carefully state Euler’s Theorem.

If $a$ and $n$ are relatively primes, then:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ is the Euler phi function of $n$.

(d) (5 points) $10^3 = 999 + 1$ and $999 = 27 \cdot 37$

Explain why this implies that 27 is not a prime number, but that
this does not tell us whether or not 37 is prime (in fact, 37 is prime).

Suppose 27 were a prime number. Then by Lagrange’s theorem, the
element $10 \in (\mathbb{Z}/27\mathbb{Z})^\times$ must have order dividing $26 = 27 - 1$ (which
would be the order of the group). But the order of 10 is 3 since:

$$10^3 \equiv 1 \pmod{27}$$

and 3 does not divide 26, so it follows that 27 is not prime!

On the other hand, 3 does divide $37 - 1 = 36$, which is consistent
with Lagrange’s theorem applied to $10 \in (\mathbb{Z}/37\mathbb{Z})^\times$. This is not enough
to conclude that 37 is a prime, however.