1. Let us define $gcd(a_1, a_2, \ldots, a_k)$ as $gcd(a_1, gcd(a_2, a_3, \ldots, a_k))$, for $k \geq 3$.

   Prove that if $gcd(a_1, a_2, \ldots, a_k) = d$, then there exist integers $x_1, x_2, \ldots, x_k$ such that $\sum_{i=1}^{k} a_i x_i = d$.

2. Prove that any two consecutive integers ($n$ and $n+1$) are always relatively prime.

3. Prove that any two consecutive Fibonacci numbers are always relatively prime.

4. Prove that two integers $a$ and $b$ are relatively prime if and only if there is no prime number $p$ such that $p \mid a$ and $p \mid b$.

5. Let $a$ and $b$ be relatively prime. Prove that, for any integer $n$, we have that both $a \mid n$ and $b \mid n$ if and only if $ab \mid n$.

6. Let $a$ and $b$ be relatively prime. Prove that, for every integer $m$, there exist integers $x$ and $y$ such that $ax + by = m$.

7. We would like to understand that relative primality was mandatory for the Chinese Remainder Theorem. Considering two integers $n$ and $m$ that are not necessarily relatively prime.

   (a) Prove that, for some $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$, it may be the case that no $x \in \mathbb{Z}_{nm}$ satisfies $x \bmod n = a$ and $x \bmod m = b$.

   (b) Prove that, for some $a \in \mathbb{Z}_n$ and $b \in \mathbb{Z}_m$, there may be more than one $x \in \mathbb{Z}_{nm}$ satisfies $x \bmod n = a$ and $x \bmod m = b$.

8. Prove or disprove: for any $n \geq 2$, there exists one and only one $b \in \mathbb{Z}_n$ such that $b^2 \equiv_n 0$.

9. Prove or disprove: for any $n \neq 2$, and for any $a \in \mathbb{Z}_n$ with $a \neq 0$, there is not exactly one $b \in \mathbb{Z}_n$ such that $b^2 \equiv_n a$.

10. Prove that the multiplicative inverse is unique: that is, for arbitrary $n \geq 2$ and $a \in \mathbb{Z}_n$, suppose that $ax \equiv_n 1$ and $ay \equiv_n 1$. Prove that $x \equiv_n y$.

11. Prove or disprove: for arbitrary $n \geq 2$, $(n-1)^{-1} = n-1$ in $\mathbb{Z}_n$.

12. Prove that $(a^{-1})^{-1} = a$ for any $n \geq 2$ and $a \in \mathbb{Z}_n$: that is, prove that a is the multiplicative inverse of the multiplicative inverse of a.

13. Prove that, for any $n \geq 2$ and $a \in \mathbb{Z}_n$, there exists $x \in \mathbb{Z}$ with $ax \equiv_n 1$ if and only if there exists $y \in \mathbb{Z}_n$ with $ay \equiv_n 1$.

14. Suppose that the multiplicative inverse $a^{-1}$ exists in $\mathbb{Z}_n$. Let $k \in \mathbb{Z}_n$ be any exponent. Prove that $a^k$ has a multiplicative inverse in $\mathbb{Z}_n$, and, in particular, prove that the multiplicative inverse of $a^k$ is the $k$th power of the multiplicative inverse of $a$. (That is, prove that $(a^k)^{-1} \equiv_n (a^{-1})^k$.)

15. Prove or disprove: if n is composite, then there exists $a \in \mathbb{Z}_n$ (with $a \neq 0$) that does not have a multiplicative inverse in $\mathbb{Z}_n$.

16. **[4 marks]** Recall the key generation protocol of RSA. Prove that:

    (a) **[2 marks]** the number $e$ that is chosen will always be odd.

    (b) **[2 marks]** the number $d$ that is chosen will always be odd.