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 $\sum_{i=1}^{k} a_i x_i = d$.

   Ans: We will prove this by induction on k. The base case (for $k = 2$) is something that we had done in the class.

   Suppose $gcd(a_2, a_3, \ldots, a_k) = d'$. By induction hypothesis, we know that that there exist integers $y_2, \ldots, y_k$ such that $\sum_{i=2}^{k} a_i y_i = d'$.

   Suppose $gcd(a_1, a_2, \ldots, a_k)$ equals d. We know that,

   $gcd(a_1, a_2, \ldots, a_k) = gcd(a_1, gcd(a_2, a_3, \ldots, a_k))$
   $= gcd(a_1, d')$

   Since this equals d, we know that we can find integers z_1 and z_2 such that

   $d = a_1 z_1 + d' z_2$

   This means that,

   $d = z_1 a_1 + z_2(\sum_{i=2}^{k} a_i y_i)$
   $= z_1 a_1 + \sum_{i=2}^{k} a_i y_i z_2$

   Substituting x_1 for z_1, and x_i for $y_i z_2$ for $2 \leq i \leq k$, we get
   $d = \sum_{i=1}^{k} a_i x_i$.

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

   Ans: If two distinct numbers have a common divisor $d \geq 1$, then the difference between those numbers must at least be d.

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

   Ans: Suppose not. Let $d > 1$ be a common divisor of F_n and F_{n+1}. Clearly, F_{n-1} must also be divisible by d (because $F_{n-1} = F_{n+1} - F_n$). Arguing similarly, d must also divide F_{n-2}. Similarly, in the other direction too. Thus, we can argue that all fibonacci numbers are divisible by d. But, we know that this is not the case (by checking the first few fibonacci numbers 1, 1, 2, 3, 5, 8, $\ldots$).

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 $p \mid b$.

   Ans: One direction is trivial.

To prove the other direction, we argue that if there is no prime number p such that $p \mid a$ and $p \mid b$, then a and b are relatively prime.

Suppose there is no prime number p such that $p \mid a$ and $p \mid b$. If a and b are not relatively prime, then there must be a composite number k such that $k \mid a$ and $k \mid b$. But then k must have a (unique) prime factorization. All those primes (in the factor) must divide both a and b. Contradiction!

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 $ab \mid n$.

   Ans: If $ab \mid n$ then n can be written as abk for some integer k. Clearly, both a and b divide abk.

   For the other direction, since a and b are relatively prime, we know that we can find integers x and y such that $ax + by = 1$. This also means that $axn + byn = n$. Since $a \mid n$, n can be written as ap for some integer p. Similarly, n can be written as bq for some integer q. Replacing the first occurrence of n by bq and the second occurrence of n by ap in $axn + byn = n$, we get $axbq + byap = n$. This implies that $ab(xq + yp) = n$, which proves that $ab \mid n$.

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

   Ans: We know that `extended-euclid` gives us integers x' and y' such that $ax' + by' = 1$. We can multiply both sides by m and get what we want.

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 $x \bmod m = b$.

   Ans: Let $n = 2, m = 4, a = 1$, and $b = 2$. There is no $x \in \mathbb{Z}_8$ such that $x \bmod 2 = 1$ and $x \bmod 4 = 2$.

   (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 $x \bmod m = b$.

   Ans: Let $n = 2, m = 4, a = 1$, and $b = 1$. There are two values of $x \in \mathbb{Z}_8$ such that $x \bmod 2 = 1$ and $x \bmod 4 = 1$, namely $x = 1$ and $x = 5$.

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

   Ans: Consider $n = 9$. Both 3^2 and 6^2 are 0 mod 9.

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 $b^2 \equiv_n a$.

   Ans: Consider $n = 6, a = 3$. There is exactly one $b \in \mathbb{Z}_6$ such that $b^2 \equiv_n 3$, namely $b = 3$.

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 $x \equiv_n y$.

    Ans: If $ax \bmod n = 1$ and $ay \bmod n = 1$, then $(ax - ay) \equiv_n 0$. This means that $(x - y)a \equiv_n 0$, which also means that $(x - y)ax \equiv_n 0$. But we know that $ax \bmod n = 1$. So $(x - y)$ must be $0 \bmod n$.

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

    Ans: Because $(n-1)(n-1)$ is $1 \bmod n$.

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.

    Ans: Suppose $b = a^{-1}$. Clearly, $b \cdot a \equiv_n 1$, which shows that $a = b^{-1}$, which is same as $(a^{-1})^{-1}$.

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 $ay \equiv_n 1$.

    Ans: This was done in the class (see the notes of Lecture n, where I can tell you that $n \bmod 5 = 2$, $n \bmod 4 = 1$).

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 kth power of the multiplicative inverse of a. (That is, prove that $(a^k)^{-1} \equiv_n (a^{-1})^k$.)

    Ans: Let x be the multiplicative inverse of a^{-1}. This means that $xa \equiv_n 1$, and therefore, $(xa)^k \equiv_n 1$. Since $x^k a^k \equiv_n 1$, the inverse of a^k is x^k, which is $(a^{-1})^k$.

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 $\mathbb{Z}_n$.

    Ans: If n is composite, there must be a $d \geq 1$ that divides n. But then d and n cannot be relatively prime, and therefore d cannot 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.

Ans: The numbers p and q are both large primes. So, they must be odd. This means that $(p-1)(q-1)$ must be even. If e is also even, then e cannot be relatively prime to $(p-1)(q-1)$.

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

Ans: We know that $d = e^{-1} \bmod (p-1)(q-1)$. Therefore, de is 1 mod $(p-1)(q-1)$. This means that de must be of the form $k(p-1)(q-1)+1$, which is odd (because $(p-1)(q-1)$ is even). But then d cannot be even.