You may assume the following facts in this quiz without proving them. But you must explicitly indicate this by writing something like "*(using fact i)*" wherever you are using the i^{th} fact from here.

1. If p is a prime number, and $a, b \in \mathbb{Z}$, then $p \mid ab$ if and only if $p \mid a$ or $p \mid b$.
2. $k^n - 1$ is evenly divisible by $k - 1$, for any $n \geq 0$ and $k \geq 2$.

1. **[1 mark]** Show that if a and b are both positive integers, then $(2^a - 1) \bmod (2^b - 1) \ = \ 2^{(a \bmod b)} - 1$.

   Ans: Let $a = bq + r$, where $r = a \bmod b$.

   $(2^a - 1) \bmod (2^b - 1)$
   $= (2^{(bq+r)} - 1) \bmod (2^b - 1)$
   $= ((2^{bq} \cdot 2^r) - 1) \bmod (2^b - 1)$
   $= (((2^{bq} - 1) \cdot 2^r) + (2^r - 1)) \bmod (2^b - 1)$
   $= (2^r - 1) \bmod (2^b - 1)$ $\quad (2^b - 1) \mid (2^{bq} - 1)$, *using fact 2 from above*
   $= (2^r - 1)$ $\quad (2^r - 1)$ is smaller than $(2^b - 1)$
   $= 2^{(a \bmod b)} - 1$

2. **[2 marks]** Show that if a and b are positive integers, then $gcd(2^a - 1, 2^b - 1) \ = \ 2^{gcd(a,b)} - 1$. Use mathematical induction.

   Ans: The claim holds trivially when a equals b. Therefore, we assume that $a > b$ (without loss of generality).

   Consider the statement

   $$P(a)\text{: } \textit{for all} \ \ 0 < b < a, \quad gcd(2^a - 1, 2^b - 1) \ = \ 2^{gcd(a,b)} - 1$$

   We will prove (using induction) that $P(a)$ holds for all $a \geq 2$.

   Base case: When $a = 2, b = 1, \quad gcd(2^a - 1, 2^b - 1) = gcd(3, 1) = 1 = 2^{gcd(2,1)} - 1 = 2^{gcd(a,b)} - 1$.

   Inductive step: We assume that $P(k)$ holds for all $2 \leq k \leq a$.
   Consider $gcd(2^{(a+1)} - 1, 2^b - 1)$. This equals
   $gcd(2^b - 1, (2^{(a+1)} - 1) \bmod (2^b - 1))$ $\quad gcd(x, y) = gcd(y, x \bmod y)$
   $= gcd(2^b - 1, (2^{(a+1) \bmod b} - 1))$ $\quad$ *from Q1, above*
   $= 2^{gcd(b,(a+1) \bmod b)} - 1$ $\quad$ from the induction hypothesis
   $= 2^{gcd((a+1),b)} - 1$ $\quad gcd(x, y) = gcd(y, x \bmod y)$

3. **[1.5 marks]** Let a and b be relatively prime. Let c be relatively prime to both a and b. Prove that c and ab are also relatively prime.

   Ans: Suppose not. Let d be an integer ≥ 2 such that $d \mid c$ and $d \mid ab$.

We know that there exist integers x and y such that

$ax + cy = 1$	*Extended-Euclid* gives us such x and y, for a and c relatively prime
implies, $abx + bcy = b$	multiplying both sides by b

Since d divides the LHS (because $d \mid ab$ and $d \mid c$), d must also divide b. But this contradicts the fact that c is relatively prime to b (because $d \geq 2$ divides both c and b).

4. **[1.5 marks]** A *palindromic bitstring* is a string of `0`'s and `1`'s that reads the same front-to-back as it does from back-to-front. For example, `0010100` is a palindromic bitstring, where `011` is not. Here is a recursive definition of palindromic bitstrings.

   - The empty string ϵ is a palindromic bitstring.
   - The string `0` (consisting of a single `0`) is a palindromic bitstring.
   - The string `1` (consisting of a single `1`) is a palindromic bitstring.
   - If `s` is a palindromic bitstring, so is `0s0`.
   - If `s` is a palindromic bitstring, so is `1s1`.

   Let $n_0(s)$ and $n_1(s)$ denote, respectively, the number of `0`'s and `1`'s in a palindromic bitstring s. Use induction to prove that $n_0(s) \cdot n_1(s)$ is even for any palindromic bitstring s.

   Ans: We will prove this by structural induction on the form of all bitstrings s.

   For the cases where s is an empty string, or a single `0` or `1`, the $n_0(s) \cdot n_1(s)$ evaluates to 0, which is even.

   When s is of the form `0x0`, $n_0(s) \cdot n_1(s)$ equals $(2 + n_0(x)) \cdot n_1(x)$, which equals $2 \cdot n_1(x) + n_0(x) \cdot n_1(x)$, which is the sum of two even numbers, and therefore even. (The first term is a multiple of 2, the second term is even by induction hypothesis – x is structurally smaller than s.)

   The case when s is of the form `1x1` is similar to the one above.