1. There’s a couple of ways of going about proving this one. People seemed to latch on to induction in class so I’ll provide a write-up of that first, followed by what I think is the easier proof via telescoping series. (Exercise to the reader: explain where $x \neq 1$ is used in each proof)

**Induction:** $n = 1$ provides the base case of $1 = \sum_{k=0}^{0} x^k = \frac{x^1 - 1}{x - 1} = 1$. Our inductive hypothesis is that the following holds for $n$:

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}.$$  

We wish to show use this hypothesis to prove the equality in the case $n + 1$. Using the hypothesis we get

$$\sum_{k=0}^{n} x^k = x^n + \frac{x^n - 1}{x - 1},$$

and we can make a common denominator to find that

$$x^n + \frac{x^n - 1}{x - 1} = \frac{x^{n+1} - x^n + x^n - 1}{x - 1} = \frac{x^{n+1} - 1}{x - 1}$$

as desired.

**Telescoping:** If we multiple both sides by $x - 1$ we get

$$x^n - 1 = \sum_{k=0}^{n-1} [x^{k+1} - x^k] = \sum_{k=1}^{n} x^k - \sum_{k=0}^{n-1} x^k = x^n - x^0 + \sum_{k=1}^{n-1} [x^k - x^k] = x^n - 1$$

as desired.

2. (a) We prove the contrapositive. For the sake of contradiction, suppose that $au + bv = 1$ and $(a, b) = d > 1$. Then $d | au + bv = 1$ since $d$ divides both $a$ and $b$. Since 1 has no divisors greater than itself, this is a contradiction, and therefore $(a, b) = 1$ as desired.

(b) This is false and there are many possible examples. For instance, $a \cdot 1 + b \cdot 1 = a + b$. If $a, b > 0$, then $(a, b) \neq a + b$ since it is larger than either $a$ or $b$. In fact, the statement in (b) almost never holds!

**Bonus problem:** Prove that if $au + bv = (a, b)$, then $(u, v) = 1$ (note this is not “if and only if”).

3. ($\Leftarrow$) Suppose $(a, n) = 1$. Then we know that $au + nv = 1$ for some $u, v \in \mathbb{Z}$. But then $au \equiv 1 \pmod{n}$ and so we have some $x \in \mathbb{Z}_n$ where $u \equiv x \pmod{n}$ such that $ax \equiv 1 \pmod{1}$ as desired.

We use a few important properties of $\mathbb{Z}_n$ implicitly here. First, we are using the fact that arithmetic in $\mathbb{Z}$ holds when restricting to congruence classes in $\mathbb{Z}_n$. Next, we’re using the fact that $u \in \mathbb{Z}$ can be used interchangeably with $[u] \in \mathbb{Z}_n$ (its corresponding conjugacy class). It’s worth taking a little bit to think about these subtleties because pretty soon we’re going to be making these kinds of assumptions without highlighting them and it’s important to start getting comfortable with that.

($\Rightarrow$) Suppose $ax \equiv 1 \pmod{n}$ for some $x \in \mathbb{Z}_n$. Then there is some $t \in \mathbb{Z}$ such that $ax + nt = 1$ by the definition of congruence. Using our result from 2 (a), we can conclude that $(a, n) = 1$.
4. We prove the contrapositive, namely, if \( p = rs > 0 \) for \( r, s > 1 \) (I’ll leave it to the reader to confirm this works for \( p < 0 \)), then there exists \( b, c \in \mathbb{Z} \) such that \( p \mid bc \) but \( p \) does not divide either of \( b \) or \( c \). Note that \( p \mid rs \) itself and, since \( r, s < p \), neither is divisible by \( p \). Therefore we have proven the desired statement by taking \( r \) and \( s \) as \( b \) and \( c \).

5. Here’s just one of the many many proofs of this result.
Suppose there were only finitely many primes and enumerate them as \( p_1 < p_2 < \cdots < p_n \). Let \( q = 1 + \prod_{k=1}^{n} p_k \). Then \( q \equiv 1 \pmod{p_i} \) for all \( 1 \leq i \leq n \). By problem 3, this implies that \( q > p_n \) is relatively prime to every prime number and hence is itself prime. This is a contradiction since we claimed there were no additional primes. Thus, we conclude there are infinitely many primes.

6. To simplify notation, we set \( r_0 = a \) and \( r_1 = b \). We claim that the following sequence of repeated applications of the Euclidean division algorithm will give the gcd as \( r_k \):

\[
egin{align*}
    r_0 &= q_1 r_1 + r_2 \\
    r_1 &= q_2 r_2 + r_3 \\
    r_2 &= q_3 r_3 + r_4 \\
    &\vdots \\
    r_{k-1} &= q_k r_k + 0.
\end{align*}
\]

Note that \( r_k \mid r_{k-1} \). Therefore \( r_{k-2} = q k_{k-1} r_{k-1} + r_k \) implies that \( r_k \mid r_{k-2} \) and in general, we use \( r_k \mid r_i, r_{i-1} \) and \( r_{i-2} = q_i r_{i-1} + r_i \) to conclude that \( r_k \mid r_{i-2} \). Therefore, by inductive descent we have that \( r_k \mid r_0, r_1 \). Thus, we have shown that \( r_k \) is a common divisor of \( r_0 \) and \( r_1 \) and we need only show that it is the greatest such. Using a similar argument to the above (exercise to the reader), we can show that \( r_k = r_0 u + r_1 v \) for some \( u, v \in \mathbb{Z} \). If \( (r_0, r_1) = d > r_k \), then we would have \( d \mid r_0 u + r_1 v = r_k \) which is a contradiction (since a positive integer can’t divide a smaller positive integer). Therefore we conclude that \( r_k = (r_0, r_1) \) as desired.

7. Suppose that \( p = ab \) for \( a, b > 1 \). Then we use exercise 1 to show

\[
2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)(\sum_{k=0}^{b-1} 2^{ak}).
\]

Both terms of this product are greater than 1 since \( a, b > 1 \). Therefore, we have shown \( 2^p - 1 \) is composite.