1. (a) The base case is $P(2)$. They start here because 1 is neither composite nor prime, and if $P(1)$ was considered in the induction, then the proof wouldn't work as you can have an infinite different number of powers of one to create different factorization of the same number.

   (b) When they define $m = (k+1)/p_1$, they use the fact that prime numbers are greater than one because otherwise, m would be greater than $k+1$.

   (c) When they use the inductive hypothesis to say m can be written as the product of primes, m never equals to $k+1-1$, so regular induction will not work. Therefore, they must use strong induction.

   (d) Since p_2 is an integer, by definition, $p_1 \mid q_1q_2$. Then by Euclid's Lemma $p_1 \mid q_1 \vee p_1 \mid q_2$. Next, assume $p_1 \mid q_1$ and $p_1 \nmid q_2$. If $p_1 \nmid q_1$, then rearrange q_1, q_2 so that it does. Since q_1 is prime, its only factors are 1 or q_1, but since p_1 is a prime but 1 is not a prime, p_1 must equal q_1. Next, dividing the equation $p_1p_2 = q_1q_2$ by either p_1 or p_2 yields $p_2 = q_2$.$\square$

2. Let a, b be arbitrary integers. Assume that $\gcd(a+3b, 5ab) = 1$. Well, by BL, $\exists x, y \in \mathbb{Z}$ such that $(a+3b)x + (5ab)y = 1$. Next, rearranging:

$$(a+3b)x + (5ab)y = 1$$
$$ax + 3bx + 5aby = 1$$
$$(x+5by)a + (3x)b = 1$$

   Since $x + 5by$ and $3x$ are both integers divisible by 1, by GCDCT, $\gcd(a, b) = 1$. $\square$

3. Let p be an arbitrary prime number. Let s, t be arbitrary natural numbers such that $s, t < p$. Well, since $s, t \neq p$, and p has no factors other than p or 1, by the CCT, $\gcd(p, s) = 1 = \gcd(p, t)$. Then, by BL, $\exists x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $px_1 + sy_1 = 1$ and $px_2 + ty_2 = 1$. Multiplying these two equations together:

$$(px_1 + sy_1)(px_2 + ty_2) = (1)(1)$$
$$p^2x_1x_2 + px_1ty_2 + sy_1px_2 + sty_1y_2 = 1$$
$$p(px_1x_2 + x_1ty_2 + sy_1x_2) + st(y_1y_2) = 1$$

   Since, $(px_1x_2 + x_1ty_2 + sy_1x_2)$ and (y_1y_2) are both integers divisible by 1, by the GCDCT, $\gcd(p, st) = 1$. $\square$

4. Note that $42^{42} = (2\cdot3\cdot7)^{42} = 2^{42}\cdot3^{42}\cdot5^0\cdot7^{42}$. Also, note that $8!^8 = (2^7\cdot3^2\cdot5\cdot7)^8 = 2^{56}\cdot3^{16}\cdot5^8\cdot7^8$. Then by the GCD PF, $\gcd(42^{42}, 8!) = 2^{42}\cdot3^{16}\cdot5^0\cdot7^8 = 2^{42}\cdot3^{16}\cdot7^8$

5. By the UFT,

$$a = p_1^{\alpha_1}\cdots p_r^{\alpha_r}, \qquad b = p_1^{\beta_1}\cdots p_r^{\beta_r}$$

   Where p_i are unique primes and $\alpha_i, \beta_i >= 0$. Allow the exponents to equal 0 if p_i occurs in one prime but not the other. We also know that $5 \nmid a$, which means we can re-write a and b as

$$a = p_1^{\alpha_1}\cdots p_r^{\alpha_r}\cdot 5^0, \qquad b = p_1^{\beta_1}\cdots p_r^{\beta_r}\cdot 5^{\beta_k}$$

   Next, by the GCDPF, $\gcd(a, b) = p_1^{\gamma_1}\cdots p_r^{\gamma_r}\cdot 5^0$, where $\gamma_r = \min(\alpha_r, \beta_r)$. We also note that that by the Euclidean algorithm $\gcd(a, a+5b) = \gcd(a, a+5b-a) = \gcd(a, 5b)$. We can now write $5b$ as

$$5b = p_1^{\beta_1}\cdots p_r^{\beta_r}\cdot 5^{\beta_k+1}$$

Then, again by GCDPF,

$$
\begin{aligned}
gcd(a, 5b) &= p_1^{\min(\alpha_1, \beta_1)} \cdots p_r^{\min(\alpha_r, \beta_r)} \cdot 5^{\min(0, \beta_k + 1)} \\
&= p_1^{\gamma_1} \cdots p_r^{\gamma_r} \cdot 5^0 \\
&= \gcd(a, b) \qquad \square
\end{aligned}
$$

6. (a) First, prove there's at least one solution:
By DA, $n = pq + r$ for some integers q, r where $0 \le r < p$. Then we must find a $k \in S$ such that $p \mid pq + r + k$.

Case 1: $r = 0$
If $r = 0$, then consider $k = 0$. Then $n + k = pq + 0 + 0 = pq$. Since $q \in \mathbb{Z}$, then by definition $p \mid pq$ which implies $p \mid n + k$.
Case 2: $r > 0$
If $r > 0$, then consider $k = p - r$. Then, $n + k = pq + r + p - r = pq + p = p(q + 1)$. Since $q + 1 \in \mathbb{Z}$, by definition, $p \mid p(q + 1)$ which implies $p \mid n + k$.

Prove that $\forall k_1, k_2 \in \mathbb{Z}$, if $p \mid n + k_1$ and $p \mid n + k_2$, then $k_1 = k_2$:
For contradiction, assume $k_1 > k_2$. Since $p \mid n + k_1$ and $p \mid n + k_2$, by DIC, $p \mid (n + k_1) - (n + k_2) = k_1 - k_2$. This implies $\exists a \in \mathbb{Z}$ such that $pa = k_1 - k_2$.

$$pa = k_1 - k_2 \tag{1}$$

$$p \le k_1 - k_2 \tag{2}$$

$$p + k_2 \le k_1 \tag{3}$$

But the condition that $0 \le k_1, k_2 < p$ implies $p + k_2 > k_1$ which is a contradiction. Therefore the assumption that $k_1 > k_2$ is false which means $k_1 \le k_2$.

The process for showing $k_1 \ge k_2$ is similar, and therefore omitted.

If $k_1 \le k_2$ and $k_1 \ge k_2$ are both true, then $k_1 = k_2$. Therefore, k is unique. $\square$

(b) From part a), there exists only one integer k in the closed interval $[0, p - 1]$ such that $p \mid n + k$. We also note that the $gcd(ap, p) = p$ for all integers a and primes p. We also note that for all integers x, where $x \neq 0$ and $p \nmid x$, $\gcd(x, p) = 1$. These are easily proven using UFT and GCD PF, but Latex is too hard and it's 2am. Then,

$$
\begin{aligned}
&\prod_{i=0}^{p-1} \gcd(n + i, p) \\
=& \gcd(n + 0, p) \cdot \gcd(n + 1, p) \cdots \gcd(n + k, p) \cdots \gcd(n + p - 1, p) \\
=& 1 \cdot 1 \cdots p \cdots 1 \\
=& p, \text{ as desired}
\end{aligned}
$$