1. For $n \in \mathbb{N}$ let P_n be the statement that $7 \mid 8^n - 1$.

Base: P_1 is the statement that $7 \mid 8^1 - 1$, which is true because $8^1 - 1 = 7 = 7 \cdot 1$.

Inductive step: Suppose $n \in \mathbb{N}$ and P_n is true, in other words there is some $k \in \mathbb{Z}$ with $8^n - 1 = 7k$. Then

$$\begin{aligned} 8^{n+1} - 1 &= 8^{n+1} - 8^n + 8^n - 1 \\ &= 8^n(8-1) + 7k \\ &= 7(8^n + k), \end{aligned}$$

so $7 \mid 8^{n+1}$, in other words P_{n+1} is true.

Hence, by induction, P_n is true for all $n \in \mathbb{N}$.

2. (a) We know that $d \in S$, so there are some $x, y \in \mathbb{Z}$ with $d = ax + by$. We also know that we can find $q, r \in \mathbb{Z}$ with $0 \le r < d$ such that $a = qd + r$. Suppose, for a contradiction, that $0 < r$. Then we have $r \in \mathbb{N}$

$$\begin{aligned} r &= a - qd \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy), \end{aligned}$$

and $1 - qx, -qy \in \mathbb{Z}$. Hence $r \in S$. But this is impossible since $r < d$ and d is the least element of S. So we cannot have $0 < r$, so $r = 0$. Thus $a = qd$, so $d \mid a$.

(b) As with part (a), we can find integers x, y, a' and r' with $0 \le r' < d$ so that $d = ax + by$ and $b = q'd + r'$. If $0 < r'$ we have

$$r = b - q'd = b - q'(ax + by) = a(-q'x) + b(1 - q'y),$$

so we would have $r' \in S$, contradicting the minimality of d. So $r' = 0$, so $b = q'd$, so $d \mid b$.

(c) Suppose $c \mid a$ and $c \mid b$. Then there exist $z, w \in \mathbb{Z}$ with $a = cz$ and $b = cw$. We also have $d = ax + by$ for some $x, y \in \mathbb{Z}$. So $d = (cz)x + (cw)y = c(zx + wy)$, and $zx + wy \in \mathbb{Z}$, so $c \mid d$.

3. (a) [In effect we are supposed to be showing that two sets are equal: the set of common divisors of a and b, and the set of common divisors of b and r. So our proof resembles a proof that two sets are equal.]

Let c be a common divisor of a and b. Then we can find $x, y \in Z$ with $a = cx$ and $b = cy$. Substituting these into $a = qb + r$ we get $cx = qcb + r$, so $r = c(x - qb)$, so $c \mid r$. Since we already knew that $c \mid b$, c is a common divisor of b and r.

Conversely, let d be a common divisor of b and r. Then there exist $z, w \in \mathbb{Z}$ with $b = dz$ and $r = dw$. Then $a = qb + r = qdz + dw = d(qz + w)$, and $qz + w \in \mathbb{Z}$, so $d \mid a$. Since we already knew that $d \mid b$, d is a common divisor of a and b.

(b) We must show that b is a common divisor of a and b, and that if c is a common divisor of a and b then $c \mid b$.

- We have $a = qb + 0$, so $a = qb$, so $b \mid a$;
- We have $b = b \cdot 1$, so $b \mid b$;
- If $c \mid a$ and $c \mid b$, then certainly $c \mid b$.

Thus $b = \gcd(a, b)$ as required.

4. (a) Euclid's Algorithm gives the following results:

55	1	0
15	0	1
10	1	-3
5	-1	4
0	3	-11

Thus $\gcd(55, 15) = 5$.

(b) From the working in (a) we see that $5 = 55 \cdot (-1) + 15 \cdot 4$. So $a = -1$, $b = 4$ is a solution.

(c) $20 = 5 \cdot 4$, so multiplying our solution of (c) by 4 gives $20 = 55 \cdot (-4) + 15 \cdot 16$. Thus $a = -4$, $b = 16$ is one solution. Also, from the working in (a) we see that $\operatorname{lcm}(55, 15) = 3 \cdot 55 = 11 \cdot 15$, so the general solution is

$$a = -4 + 3t, \qquad b = 16 - 11t,$$

for $t \in \mathbb{Z}$.

(d) We have $5 \mid 55$ and $5 \mid 15$, so $5 \mid 55a+15b$ for any $a, b \in \mathbb{Z}$. However, $5 \nmid 23$. Thus $55a+15b = 23$ has no integer solutions.