Exercise 5 a) Base case: $k = 2$. Suppose $a_1 | b$, $a_2 | b$ and $\gcd(a_1, a_2) = 1$.

Then $\ell cm(a_1, a_2) = a_1 a_2$ so $a_1 a_2 | b$ because the least common multiple must divide every other common multiple.

Induction hypothesis: If $\gcd(a_i, a_j) = 1$ for $1 \leq i < j \leq k$

and $a_i | b$ for $i = 1, \ldots, k$ then $\prod_{i=1}^{k} a_i | b$.

Induction step: Suppose $\gcd(a_i, a_j) = 1$ for $1 \leq i < j \leq k+1$

and $a_i | b$ for $i = 1, \ldots, k, k+1$. Then $\prod_{i=1}^{k} a_i | b$ by the hypothesis

But $\gcd(\prod_{i=1}^{k} a_i, a_{k+1}) = 1$ by Exercise 4 so $\prod_{i=1}^{k+1} a_i | b$ by the result for $k = 2$.

Exercise 6 b) Here we apply the extended Euclidean algorithm:

STEPS	q_3	r	x_3	y_3	a	b	x_2	x_1	y_2	y_1
2					3587	1819	0	1	1	0
1st 3	1	1768	1	−1	1819	1768	1	0	−1	1
2nd 3	1	51	-1	2	1768	51	-1	1	2	-1
3rd 3	34	34	35	−69	51	34	35	−1	−69	2
4th 3	1	17	−36	71	34	17	−36	35	71	−69
5th 3	2	0			17	0		-36		71

so $d = 17$, $x = -36$, $y = 71$

Check: $\frac{3587}{17} = 211$, $\frac{1819}{17} = 1$

$$(3587)(-36) + (1819)(71) = -129132 + 129\,149 = 17$$

Exercise 7 Write $a = q_1^{e_1} \cdots q_k^{e_k}$ where $q_1, \cdots, q_k$ are primes and each $e_i \geq 1$ (This is so because $p^t | a$ forces $a \geq 2$)

Now $p^t | q_1^{e_1} \cdots q_k^{e_k}$

implies $\exists$ i such $p^t | q_i^{e_i}$ which, in turn forces $p = q_i$. But then $p^t | p^{e_i}$ implies $t \leq e_i$ or else $p^t > p^{e_i}$.

Exercise 8. $x = \hat{q}\, n + \hat{r}$

and $0 \leq \hat{r} < n$

If $\hat{r} = 0$ then $x = (\hat{q} - 1)\, n + n$ so $q = \hat{q} - 1$ and $r = n$ will suffice. If $\hat{r} > 0$ so that $1 \leq r = \hat{r} \leq n$ we can use $q = \hat{q}$ and $r = \hat{r}$.

As for uniqueness, suppose $x = q_1\, n + r_1 = q_2 n + r_2$ where $1 \leq r_1, r_2 \leq n$.

Assuming $r_2 \geq r_1$ we get $r_2 - r_1 < n$. But $(q_1 - q_2)\, n = r_2 - r_1$ so $r_2 - r_1 = 0$ and $r_1 = r_2$, which also forces $q_1 = q_2$.

Exercise 9 b) By 4) $\varphi(p^e) = p^e \left(1 - \frac{1}{p}\right)$

gcd(m, n) = 1 we may write

$m = q_1^{e_1} \cdots q_k^{e_k}$ and $n = p_1^{f_1} \cdots p_\ell^{f_\ell}$ where $q_i \neq p_j \ \forall i, j$.

Thus $m\, n = q_1^{e_1} \cdots q_k^{e_k} p_1^{f_1} \cdots p_\ell^{f_\ell}$ and

$$\varphi(mn) = m\, n \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_k}\right)\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right) = \varphi(m)\varphi(n)$$

Exercise 9 a) Consider

$$1 \le i_1 < i_2 < \cdots < i_t \le k$$

and

$$m \in \bigcap_{j=1}^{t} A_{i_j}$$

Observe

$$m \in \bigcap_{j=1}^{t} A_{i_j} \quad \Leftrightarrow \quad p_{i_1} p_{i_2} \cdots p_{i_t} \mid m$$

$$\Leftrightarrow \quad p_{i_1} p_{i_2} \cdots p_{i_t} \ \alpha = m$$

for

$$\alpha \le \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_t}} = \prod_{j=1}^{t} p_{i_j}^{e_{i_j}-1} \prod_{j \ne j_i} p_j^{e_j}$$

Therefore

$$\left| \bigcap_{j=1}^{t} A_{i_j} \right| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_t}}$$

Now

$$\left| \bigcap_{j=1}^{k} A_j^e \right| = \left| [n] \right| - \left| \bigcup_{j=1}^{k} A_j \right|$$

$$= n - \sum_{t=1}^{k} (-1)^{t+1} \sum_{i_1 < \cdots < i_t} \left| \bigcap_{j=1}^{t} A_{i_j} \right|$$

$$= n \left(1 + \sum_{t=1}^{k} (-1)^t \frac{1}{p_{i_1} \cdots p_{i_t}} \right)$$

$$= n \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i} \right) \right)$$

Exercise 9 c)

$\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = \varphi(2^2) = 2^2 - 2 = 2$

$\varphi(5) = 4$

$\varphi(6) = \varphi(3)\varphi(2) = 2$

$\varphi(7) = 6$

$\varphi(8) = \varphi(2^3) = 8 - 4 = 4$

$\varphi(9) = \varphi(3^2) = 9 - 3 = 6$

$\varphi(10) = \varphi(5)\varphi(2) = 4$

$\varphi(11) = 10$

$\varphi(12) = \varphi(2^2)\varphi(3) = (2)(2) = 4$