1a Since $a^n = e$, a has finite order.

Let $k = |a|$. By the division algorithm

$\exists!\, q, r \in \mathbb{Z}$ $n = kq + r$, $0 \le r < k$

Then $a^r = a^{n-kq} = a^n \cdot (a^k)^{-q} = e \cdot e^{-q} = e$.

Since $r < k$, $r = 0$ ◡̈

1b (i) Let $m = |a|$, $n = |b|$, $\ell = \operatorname{lcm}(m, n)$.

Since $m \mid \ell$ & $n \mid \ell$, $\exists\, m', n'$ $\ell = mm' = nn'$.

Since a and b commute,

$$(ab)^\ell = a^\ell b^\ell = (a^m)^{m'} \cdot (b^n)^{n'} = e^{m'} \cdot e^{n'} = e$$

(ii) Suppose $(ab)^k = e$. Then $a^k b^k = e$, so $a^k = b^{-k}$.

Since $a^k \in \langle a \rangle$, $b^{-k} \in \langle b \rangle$,

and $\langle a \rangle \cap \langle b \rangle = \{e\}$, $a^k = b^{-k} = e$, so $b^k = e$.

By part (a), $m \mid k$ & $n \mid k$, so $\ell \mid k$.

(so $\ell \le k$)

(iii) Thus, $|ab| = \ell$ ◡̈

2a (i) $0 = k \cdot 0 \in k\mathbb{Z}$

(ii) If $km, kn \in k\mathbb{Z}$, $km - kn = k(m-n) \in k\mathbb{Z}$

Alternate proof: $k\mathbb{Z} = \ker \pi$, where $\pi : \mathbb{Z} \to \mathbb{Z}_k$
is the natural projection $(\pi(x) = x \bmod k)$

2b (i) Since H is nontrivial, $\exists\, n \in H$, $n \neq 0$.

Let $S = \{ j \in H : j > 0 \}$.

If $n > 0$, $n \in S$. If $n < 0$, $-n \in S$.

$\therefore$ $S \neq \phi$, so by the well ordering principle

S has a minimum. Let $k = \min S$.

(ii) Since $H < \mathbb{Z}$, $k\mathbb{Z} \subseteq H$.

(iii) Conversely, suppose $h \in H$.

By the division algorithm $\exists!\, q, r$ $h = kq + r$, $0 \le r < k$

Then by (ii) $r = h - kq \in H$.

Since $0 \le r < k$, $r \notin S$, so $r = 0$.

Thus, $h = kq \in k\mathbb{Z}$. ☺

3a $\varphi : \mathbb{Z}_{35} \to \mathbb{Z}_{14}$, $\varphi(4) = 12$

Since $9 \cdot 4 \equiv 1 \bmod 35$,

$$\varphi(1) = \varphi(9 \cdot 4) = 9\,\varphi(4) = 9 \cdot 12 \equiv 10 \bmod 14$$

$$\varphi(x) = \varphi(x \cdot 1) = x\,\varphi(1) = 10x$$

3b image of $\varphi = 10 \cdot \mathbb{Z}_{14} = \{0, 10, 6, 2, 12, 8, 4\}$ $\quad |\text{image}| = 7$

$$10x \equiv 0 \bmod 14 \iff 5x \equiv 0 \bmod 7$$
$$\iff 3 \cdot 5x \equiv 0 \bmod 7$$
$$\iff x \equiv 0 \bmod 7$$

$\therefore$ $\ker \varphi = 7\mathbb{Z}_{35} = \{0, 7, 14, 21, 28\}$ $\quad |\ker| = 5$

```
(%i1)   create_list([x,mod(inv_mod(4,35)·12·x,14)],x,0,35−1);
(%o1)   [[0,0],[1,10],[2,6],[3,2],[4,12],[5,8],[6,4],[7,0],[8,10],[9,6],[10,2],[11,12],
[12,8],[13,4],[14,0],[15,10],[16,6],[17,2],[18,12],[19,8],[20,4],[21,0],[22,10],[23,6],
[24,2],[25,12],[26,8],[27,4],[28,0],[29,10],[30,6],[31,2],[32,12],[33,8],[34,4]]
```

Relationship: $|G| = |\text{image}| \cdot |\ker|$ $\quad (35 = 7 \cdot 5)$

(i) $y \in \text{image} \iff \varphi^{-1}(\{y\}) \neq \emptyset$, so the number of nonempty fibers is the size of the image.

(ii) If $x \in \varphi^{-1}(\{y\})$, $\varphi(x) = y$ and $\varphi^{-1}(\{y\}) = x + \ker\varphi$

Pf: $\varphi(z) = y \iff \underbrace{\varphi(z - x)}_{\varphi(z) - y} = 0 \iff z - x \in \ker\varphi$

$$\iff z = x + \ker\varphi$$

Thus, nonempty fibers are shifts of the kernel so have the same size as the kernel.

(iii) Nonempty fibers partition G [notes 9/8 p. 5]

so $|G| = \#$ of nonempty fibers $\times$ size of each fiber

$$= |\text{image}| \cdot |\ker|$$:)