1. Since f is surjective and the assumption '$g \circ f$ is injective' implies that f is injective, we get that f is bijective. Hence, f has an inverse function$f^{-1}\colon B \to A$, which is also bijective. This implies that $g = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1}$ is injective (as both $g \circ f$ and f^{-1} are).
2. Call the given statement $\mathcal{S}(n)$. $\mathcal{S}(0)$ holds, because if A and $m \in \mathbb{N}$ are such that there exist (i) an injective $f\colon A \to 0 = \emptyset$ and (ii) a bijective $g\colon A \to m$, then $A = \emptyset$ from (i) and hence $m = \emptyset = 0$ from (ii), so $m = 0 \le 0 = n$. Assume now that $\mathcal{S}(n)$ holds. To prove $\mathcal{S}(n')$, consider any A and $m \in \mathbb{N}$, and injective $f\colon A \to n'$ and bijective $g\colon A \to m$. If $A = \emptyset$, then $m = 0$ as before, and $m = 0 \le n'$. Assume $A \ne \emptyset$, and fix $a \in A$. Hence $m \ne 0$, and therefore $m = k'$ for some $k \in \mathbb{N}$. By HW2,Pr1, we may assume (by replacing f by $\bar{f}$ and g by $\bar{g}$) that $f(a) = n\,(\in n')$ and $g(a) = k\,(\in k')$. Applying the induction hypothesis to the restrictions of the functions f and g to $A \setminus \{a\}$, we get that $k \le n$. Hence, $k' \le n'$.
3. Let $d = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$. Clearly, $d \mid a$, because $a = dq$ for $q = p_1^{k_1-m_1} p_2^{k_2-m_2} \dots p_r^{k_r-m_r}$ where $q \in \mathbb{Z}$ (as all $k_i - m_i \in \mathbb{N}$). Similarly, $d \mid b$. Assume now that $c \mid a, b$ ($c \in \mathbb{Z}$). Then $c \ne 0$ and $-c \mid a, b$, so we may assume $c \in \mathbb{N} \setminus \{0\}$. Thus, c has a prime factorization $c = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r} q_1^{v_1} \dots q_s^{v_s}$ where $q_1, \dots, q_s$ are distinct primes different from $p_1, \dots, p_r$, and all $u_i, v_i \in \mathbb{N}$. Since $c \mid a$, we have $a = c\tilde{q}$ for some $\tilde{q} \in \mathbb{N} \setminus \{0\}$. Replacing c and $\tilde{q}$ by their prime factorizations, we get a new prime factorization for a, which may differ from the original one only in the order of its factors. Thus, $v_1 = \cdots = v_s = 0$ and $u_i \le k_i$ for all i ($1 \le i \le r$). The same argument for b yields also that $u_i \le \ell_i$ for all i ($1 \le i \le r$), and hence $u_i \le m_i$ for all i ($1 \le i \le r$). Thus, $c \mid cp_1^{m_1-u_1} p_2^{m_2-u_2} \dots p_r^{m_r-u_r} = d$.
4. (a) Since $o(a) = 1932$, $\langle a^{294} \rangle = \langle a^{\gcd(294,1932)} \rangle = \langle a^{42} \rangle$, and similarly, $\langle a^{189} \rangle = \langle a^{\gcd(189,1932)} \rangle = \langle a^{21} \rangle$. Now $a^{42} = (a^{21})^2 \in \langle a^{21} \rangle$ implies $a^{42} \in \langle a^{21} \rangle$, and hence $\langle a^{294} \rangle = \langle a^{42} \rangle \subseteq \langle a^{21} \rangle = \langle a^{189} \rangle$. Note: It follows also that $o(a^{189}) = o(a^{21}) = \frac{1932}{21} = 92$.
(b) $a^{294} = (a^{189})^k$ ($k \in \mathbb{Z}$) iff $1932 \mid 189k - 294$ iff $189k + 1932(-q) = 294$ for some $q \in \mathbb{Z}$. Since $21 | 189, 1932, 294$, this equation is equivalent to $9k + 92(-q) = 14$. Using the Euclidean algorithm, one can find $s, t \in \mathbb{Z}$ satisfying $9s + 92t = \gcd(9, 92) = 1$: say, $s = 41$, $t = -4$. Hence $k = 14 \cdot 41 = 574$ and $q = -14(-4) = 56$ satisfy $9k + 92(-q) = 14$. Thus, $k = 574$ works, but so does any integer $\equiv 574 \pmod{92}$ (where $92 = o(a^{189})$), say $k = 22$.
5. (a) $(ab)^2 = a^2b^2 \Leftrightarrow abab = aabb \overset{!}{\Leftrightarrow} ba = ab$ where $\Rightarrow$ is obtained in $\overset{!}{\Leftrightarrow}$ by multiplying both sides by a^{-1} on the left and b^{-1} on the right, while $\Leftarrow$ is obtained in $\overset{!}{\Leftrightarrow}$ by multiplying both sides by a on the left and b on the right.
(b) If $g^2 = e$ for all $g \in G$, then for any $a, b \in G$ we have $(ab)^2 = e = ee = a^2b^2$, and hence $ab = ba$ (by part (a)). Thus, G is abelian.
6. Let $\pi = \gamma_1 \gamma_2 \dots \gamma_m$ be the cycle decomposition of π. Since $\gamma_1, \gamma_2, \dots, \gamma_m$ are disjoint cycles, they commute, and hence for every integer k, $\pi^k = \gamma_1^k \gamma_2^k \dots \gamma_m^k$. We saw in Pr3,Wsh2 that $o(\gamma_i)$ is the length ℓ_i of the cycle γ_i for every i, so $\gamma_i^{\ell_i} = \mathrm{id}$ and $\gamma_i^k = \mathrm{id}$ whenever $\ell_i \mid k$; however, if $\ell_i \nmid k$, then γ_i^k fixes none of the elements that occur in γ_i. Therefore, $\pi^k = \mathrm{id}$ iff $\ell_i \mid k$ for all i iff $\mathrm{lcm}(\ell_1, \ell_2, \dots, \ell_m) \mid k$. Hence, $o(\pi) = \mathrm{lcm}(\ell_1, \ell_2, \dots, \ell_m)$.
7. (a) No such example exists. If a surjective, non-injective function $g\colon A \to A$ existed for a finite set A, then by assigning to each $a \in A$ a $b \in A$ such that $g(b) = a$, we would get an injective, non-surjective function $A \to A$, contradicting Cor.1.5(6) in Lec.Notes 02/03.
(b) No such a, b exist. See Pr2,HW3 if $a, b \ne 0$. If $0 \in \{a, b\}$, say $a = 0$, then $0 = \mathrm{lcm}(a, b)$.
(c) Example: $\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$.
(d) Example 1: $\pi = \sigma = (1\ 2)$, $\pi\sigma = \mathrm{id}$. Example 2: $\pi = (1\ 2\ 3\ 4)$, $\sigma = (1\ 3\ 2)$, $\pi\sigma = (1\ 4)$.
(e) No such $G = \langle a \rangle$ exists, because $a^k a^\ell = a^{k+\ell} = a^\ell a^k$ for all $a^k, a^\ell \in \langle a \rangle$.
(f) No such $\pi \in S_n$ exists. Indeed, if σ is odd, i.e., it is a product of an odd number of transpositions, say m, then for every $k \in \mathbb{Z}$, σ^k is a product of mk transpositions. Hence, σ^k is odd if k is odd. Since id is even, $\sigma^k \ne \mathrm{id}$ if k is odd.