d) We apply (c) to $\langle g^i \rangle = G = \langle g^1 \rangle$ and obtain $\gcd(m,i) \mid 1$ which means $\gcd(m,i) = 1$.

Example: Inspection of $\mathbb{Z}_{12}$:

a) generators are $1, 5, 7, 11$.

b) There exist subgroups of order $1, 2, 3, 4, 6, 12$ these are generated by $12, 6, 4, 3, 2, 1$ in turn.

c) of course there are alternative generators for the subgroups. For example $\langle 2 \rangle = \langle 10 \rangle$ and $\langle 4 \rangle = \langle 8 \rangle$.

d) Asking, if $\langle 8 \rangle \subseteq \langle 10 \rangle$ leads to $\gcd(12,10) \mid 8$ which is true.

Def: For a group G and an arbitrary element $a \in G$ consider the left multiplier $l_a : G \to G$, $x \mapsto ax$ and the right multiplier $r_a : G \to G$, $x \mapsto xa$.

Lemma. r_a and l_a are bijections of G.

proof $(r_a)^{-1} = r_{a^{-1}}$ and $(l_a)^{-1} = l_{a^{-1}}$, which finishes the proof.

Def. Let G be a group and $a \in G$, and let H be a subgroup of G. The left cosets and the right cosets of H in G are defined as

$$aH = l_a(H) \quad \text{and} \quad Ha = r_a(H)$$

and we define the sets of cosets as

$$L(H) = \{aH \mid a \in G\} \text{ and}$$
$$R(H) = \{Ha \mid a \in G\}.$$

Lemma: $|L(H)| = |R(H)|$ in the finite and infinite case

Proof: $\varphi : L(H) \to R(H)$, $aH \mapsto Ha^{-1}$ is well-defined and a bijection. Bijection is clear, once the well-definedness is assured. For this, let $aH = bH$ for some $a, b \in G$. Then there exists $h \in H$ with $a = bh$, and hence $a^{-1} = h^{-1}b^{-1}$. From this we obtain

$$Ha^{-1} = H(h^{-1}b^{-1}) = (Hh^{-1})b^{-1} = Hb^{-1}.$$

Def. Let G be a group and $H \leq G$. We define the index of H in G as $[G : H] = |L(H)| = |R(H)|$.

Lemma: Any two left cosets are disjoint or they will co-incide.

This means $aH \cap bH \neq \emptyset \Rightarrow aH = bH$.

The same is true for right cosets.

Proof. Assume $aH \cap bH \neq \emptyset$, Then there is x in this intersection and hence $x = au$ for some $u \in H$ and $x = av$ for some $v \in H$.

This yields $aH = auH = xH = bvH = bH$,

where like earlier, we have used that $hH = H$ for every $h \in H$.

Theorem (Lagrange) Let G be a finite group and let H be a subgroup of G.

Then $[G : H] \cdot |H| = |G|$.

proof: Let $L(H) = \{a_1H, a_2H, \dots, a_nH\}$ where $n = [G : H]$. We have $|G| = |\bigcup_{i=1}^{n} a_iH|$

$$= \sum_{i=1}^{n} |a_iH| = \sum_{i=1}^{n} |H| = n \cdot |H| = [G:H] \cdot |H|.$$

The only thing that should be noted is the first equality, which comes from the fact that

$$G = \bigcup_{a \in G} aH = \bigcup \{aH \mid aH \in L(H)\} = \bigcup_{i=1}^{n} a_iH. \quad \square$$

Remark. a) The proof can in the same way be done for the right cosets.

b) $[G : H]$ can be finite even if H and G are infinite.

Corollary: Let G be a finite group and let $g \in G$.

a) $|g| \mid |G|$.

b) $g^{|G|} = e$

c) $|G|$ prime $\Rightarrow$ G cyclic

Proof: a) $\langle g \rangle$ is a subgroup of order $|g|$ and hence $|g|$ is a divisor of $|G|$ by Lagrange

b) $g^{|g|} = e$, and as $|G|$ is a multiple of $|g|$ we find $g^{|G|} = e$

c) In G the elements can only have order 1 or p when $p = |G|$ is prime. Hence for each $g \neq e$ there holds $\langle g \rangle = G$,

Theorem: (Fermat's little theorem)
Let $a \in \mathbb{Z}$ with $p \nmid a$ where p is a prime number. Then $a^{p-1} \equiv 1 \pmod{p}$.

proof: Reduce a mod p to assume that $a \in \{1, \dots, p-1\}$ without loss of generality. Then $a \in \mathbb{Z}_p^*$ which is a group of order $p-1$ with respect to multiplication. For this reason $a^{p-1} \equiv e$, which means $a^{p-1} \equiv 1 \pmod{p}$

Lemma: Let G be a group such that $x^2 = e$ for all $x \in G$. Then G is abelian.

proof. We have for $x, y \in G$ the equation

$$xyxy = (xy)^2 = e = x^2y^2 = xxyy.$$

From this we deduce $yx = xy$.

proposition. All groups G with $|G| \leq 5$ are known and particularly abelian.

For the prime orders, we have cyclic groups of order $2, 3, 5$. The trivial group of order 1. For $|G| = 4$ we have 2 avenues. If there exists an element of order 4, then the group G is cyclic. Otherwise $x^2 = e$ for all $x \in G$. But then G is abelian and we can write G additively to see that $2x = 0$ for all $x \in G$. In this case G is an $\mathbb{F}_2$-vector space of dimension 2, which means G is the same as $\mathbb{F}_2^2$. Alternatively with a Cayley table

	e	a	b	c
e	e	a	b	c
a	a	e	①	②
b	b	③	e	⑤
c	c	④	⑥	e

① must be c
② must be b
③ " " c
④ " " b
⑤ & ⑥ must be a.