Exercises, week 11.

This exercise sheet is made to be done in order. In particular, one should often refer to Exercise k to do Exercise n with $k < n$.

We recall the more general Bezout identity.

Theorem 1: Let $n, m \in \mathbb{Z}$, then there exists $\alpha, \beta \in \mathbb{Z}$ such that

$$\alpha n + \beta m = \gcd(n, m).$$

Recall also that for a finite group G, we the cardinality of G is called its order.

Exercise 1: Let $(G, \cdot)$ be a finite group, let $x \in G$ of order n. Let $k > 0$,

1. Prove that $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$.
2. Prove that $\mathrm{ord}(x^{\gcd(n,k)}) = \frac{n}{\gcd(n,k)}$.
3. Conclude that $\mathrm{ord}(x^k) = \frac{n}{\gcd(n,k)}$.
4. Let $k \in \mathbb{Z}/n\mathbb{Z}$, prove that $\gcd(k, n) = 1$ if and only if k is a generator of $\mathbb{Z}/n\mathbb{Z}$.

Exercise 2: Let $(G, \cdot, e)$ be a cyclic group, generated by x. Let $H \subset G$ be a subgroup.

1. Assume $H = \{e\}$. Show that H is a cyclic group.

Assume now that $H \neq \{e\}$.

2. Show that the set $\{n > 0 \mid x^n \in H\}$ is not empty.
3. Call $m := \min\{n > 0 \mid x^n \in H\}$. Show that $H = \langle x^m \rangle$.
4. Conclude that all subgroup of a cyclic group are cyclic.

Exercise 3: Let $(G, \cdot, e)$ be a cyclic group, generated by x. Let $n = |G|$, let d be a divisor of n.

1. Show that $\langle x^{\frac{n}{d}} \rangle$ is a subgroup of G of order d.
2. Let H be a subgroup of G of order d. Show that $H = \langle x^{\frac{n}{d}} \rangle$ (hint: Exercise 2).
3. Find all the subgroups of G.

Exercise 4: Find all the subgroup of $\mathbb{Z}/12\mathbb{Z}$.

Exercise 5: Recall Euler's totient function, defined by

$$\phi(n) := |\{k \mid 1 \leq k \leq n, \gcd(k, n) = 1\}|.$$

Let G be a cyclic group of order n, generated by x. Let d be a divisor of n.

1. Let H be the only subgroup of G of order d. Suppose $z \in G$ with $\mathrm{ord}(z) = d$, show that $z \in H$.
2. Deduce that G has $\phi(d)$ many elements of order d.
3. Show that
$$G = \sum_{d|n} \{z \mid \mathrm{ord}(z) = d\},$$
and that the union is disjoint.
4. Conclude by proving that
$$n = \sum_{d|n} \phi(d).$$