HOMEWORK ASSIGNMENTS

1. Week 1

1. Find all $x \in \mathbb{Z}$ such that $3x + 7$ is divisible by 11.
2. Suppose $a, b, n \in \mathbb{Z}$. Prove that if $\gcd(a, n) = \gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.
3. Suppose m and n are two positive integers. Prove that $f : \mathbb{Z}_n \to \mathbb{Z}_m, f([x]_n) := [x]_m$ is a well-defined function if and only if $m|n$.
4. Find all the solutions of $[14]_{21}[x]_{21} = [28]_{21}$.
5. Let n be a positive integer. For a positive divisor d of n, let
$$A_d := \{k \in \mathbb{Z} \mid 1 \leq k \leq n, \gcd(k, n) = d\}.$$
   (a) Prove that $|A_d| = \phi(\frac{n}{d})$.
   (hint. $\gcd(k, n) = d$ iff $\gcd(\frac{k}{d}, \frac{n}{d}) = 1$, and $\phi(m) = |\{\ell \in \mathbb{Z} \mid 1 \leq \ell \leq m, \gcd(\ell, m) = 1\}|$.)
   (b) Prove that $\sum_{d|n, d>0} \phi(\frac{n}{d}) = n$.
   (hint. Notice that $\{A_d \mid d|n, d > 0\}$ is a partition of $\{1, \ldots, n\}$.)

2. Week 2

1. Use Euclid's algorithm to write $\gcd(198, 47)$ as an integer linear combination of 198 and 47.
2. Suppose $(G, \cdot)$ is a group and $x, y \in G$. Suppose $x^n = y^n$ and $x^m = y^m$ for some non-zero integers m, n such that $\gcd(m, n) = 1$. Prove that $x = y$. (hint. notice that there are integers r and s such that $rm + sn = 1$.)
3. Suppose $(G, \cdot)$ is a group and for every $g \in G$, $g^2 = e_G$ where e_G is the neutral element of G. Prove that G is abelian; that means for every $x, y \in G$, $x \cdot y = y \cdot x$.
4. Suppose $\mathcal{G}$ is an infinite path whose vertices are integer points and $i \in \mathbb{Z}$ is connected to exactly two points $i - 1$ and $i + 1$. Let $\sigma : \mathbb{Z} \to \mathbb{Z}, \sigma(x) := x + 1$ and $\tau : \mathbb{Z} \to \mathbb{Z}, \tau(x) := -x$.
   (a) Prove that σ and τ are symmetries of $\mathcal{G}$.
   (b) Prove that if γ is a symmetry of $\mathcal{G}$ and $\gamma(0) = 0$ and $\gamma(1) = 1$, then γ is the identity map.
   (c) Prove that if γ is a symmetry of $\mathcal{G}$, $\gamma(0) = 0$, $\gamma(1) = -1$, then $\gamma = \tau$.
   (d) Prove that $\mathrm{Sym}(\mathcal{G}) = \{\sigma^i \mid i \in \mathbb{Z}\} \cup \{\sigma^i \circ \tau \mid i \in \mathbb{Z}\}$.

3. Week 3

1. Suppose $f : G \to H$ is a group homomorphism. Prove that f is injective if and only if $\ker f = \{e_G\}$ where e_G is the neutral element of G.
2. Suppose $(G, \cdot)$ is a group and $g, x, y \in G$. Prove that $x \cdot g \cdot x^{-1} = y \cdot g \cdot y^{-1}$ if and only if $x^{-1} \cdot y \in C_G(g)$.
3. Suppose $(G, \cdot)$ is a group. An *automorphism* of G is a bijective group homomorphism $f : G \to G$. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$. The set $\mathrm{Aut}(G)$ can be viewed as the group of *symmetries* of G. Convince yourself that $(\mathrm{Aut}(G), \circ)$ is a group where $f_1 \circ f_2$ is the composite of two automorphisms f_1 and f_2.
   (a) Prove that for every $g \in G$, $c_g : G \to G, c_g(x) := g \cdot x \cdot g^{-1}$ is an automorphism of G.
   (b) Let $c : G \to \mathrm{Aut}(G), c(g) := c_g$. Prove that c is a group homomorphism.
   (c) Prove that $\ker c = Z(G)$.
4. Suppose m and n are two positive integers and $\gcd(m, n) = 1$. Let
$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, f([x]_{mn}) := ([x]_m, [x]_n).$$
   (a) Use problem 3, week 1, to show that f is a well-defined function.

(b) Prove that for an integer x, $m|x$ and $n|x$ if and only if $mn|x$. (hint. let $x = mk$ for some integer k. Since $n|mk$ and $\gcd(n, m) = 1$, by Euclid's lemma $n|k$.)
(c) Prove that f is injective.
(d) Prove that f is surjective. (hint. notice that $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$.)
(e) Prove that f is a group homomorphism.
(f) Prove that $[x]_{mn} \in \mathbb{Z}_{mn}^\times$ if and only if $f([x]_{mn}) \in (\mathbb{Z}_m^\times) \times (\mathbb{Z}_n^\times)$.
(g) Prove that $\phi(mn) = \phi(m)\phi(n)$.

4. Week 4

1. Suppose G is a finite abelian group, $a, b \in G$, and $\gcd(o(a), o(b)) = 1$.
   (a) Prove that $\langle a\rangle \cap \langle b\rangle = \{e_G\}$. (Hint. Argue that $|\langle a\rangle \cap \langle b\rangle|$ divides $|\langle a\rangle|$ and $|\langle b\rangle|$. This can be done either using the fact that there is a bijection between subgroups of a cyclic group and positive divisors of its order, or Lagrange's theorem.)
   (b) Prove that $o(ab) = o(a)o(b)$. (Hint. suppose $(ab)^m = e_G$ if and only if $a^m = b^{-m}$. In this case, they are in $\langle a\rangle \cap \langle b\rangle$.)
   (c) Prove that $a \in \langle ab\rangle$. (Hint. Consider $(ab)^{o(b)}$.)
   (d) Prove that $\langle ab\rangle = \langle a, b\rangle$; in particular, $\langle a, b\rangle$ is a cyclic group.
2. Suppose G is a finite group of order n, and for every positive integer m the equation $x^m = e_G$ has at most m solutions in G. For every integer d, let $\Psi(d)$ be the number of elements of G that have order d.
   (a) Prove that if $\Psi(d) \neq 0$, then $\Psi(d) = \phi(d)$ where ϕ is the Euler-phi function.
   (b) Use the fact that order of every element of g divides n to show that $\sum_{d|n, d\geq 1} \Psi(d) = n$.
   (c) Use the previous parts and problem 5, week 1, to show that $\Psi(d) = \phi(d)$ if $d|n$ and $d \geq 1$.
   (d) Prove that G is a cyclic group.
3. Let $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 5 & 1 & 6 & 9 & 10 & 8 & 7 \end{pmatrix} \in S_{10}$.
   (a) Find a cycle decomposition of σ.
   (b) Find out whether σ is odd or even.
   (c) Find a cycle decomposition of σ^2.
   (d) Find $o(\sigma)$.
   (e) Find $o(\tau\sigma^{18}\tau^{-1})$, where $\tau \in S_{10}$.