Math 3140 - Assignment 2

Due September 10, 2021

(1) Let G be a group, let $g, h \in G$. Show that
$$(gh)^{-1} = h^{-1}g^{-1}.$$
(2) Let $n \in \mathbb{N}, a, a', b, b' \in \mathbb{Z}$ such that $a \equiv_n a', b \equiv_n b'$. Show
$$a + b \equiv_n a' + b'.$$
(3) Use the Euclidean algorithm to find $\gcd(a, b)$ and Bezout's coefficients $u, v \in \mathbb{Z}$ such that
$$u \cdot a + v \cdot b = \gcd(a, b)$$
for $a = 51, b = 36$.

(4) Compute the following multiplicative inverses in $\mathbb{Z}_n$ if possible:
  (a) $[12]^{-1}$ in $\mathbb{Z}_{35}$
  (b) $[14]^{-1}$ in $\mathbb{Z}_{35}$

  Hint: Use the Euclidean Algorithm to compute Bezout's coefficients.

(5) Let $n \in \mathbb{N}, n > 1$. We call $[a] \in \mathbb{Z}_n$ a *zero-divisor* if there exists some nonzero $[b] \in \mathbb{Z}_n$ such that $[a] \cdot [b] = [0]$.
  (a) What are the zero divisors in $\mathbb{Z}_6$?
  (b) Show that $[a]$ is a zero divisor in $\mathbb{Z}_n$ if $\gcd(a, n) \neq 1$.
  (c) True or false? Every element in $\mathbb{Z}_n$ is either invertible or a zero-divisor.

(6) For $n \in \mathbb{N}$, let $\mathbb{Z}_n^*$ denote the set of elements in $\mathbb{Z}_n$ that have a multiplicative inverse. Show that $(\mathbb{Z}_n^*, \cdot)$ is a group.

  Hint: Don't forget to show that $\cdot$ is an operation on $\mathbb{Z}_n^*$, i.e., that the product of invertible elements is invertible again.