Math 3140 - Assignment 2

Due September 7, 2016

(1) Find the cycle decomposition for the perfect in-shuffle for $4, 6, 12$ cards, respectively. What are their orders?

(2) Let $n \in \mathbb{N}, a, a', b, b' \in \mathbb{Z}$ such that $a \equiv_n a', b \equiv_n b'$. Show

$$a + b \equiv_n a' + b',$$
$$a \cdot b \equiv_n a' \cdot b'.$$

(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) $a = 29, b = 13$,
 (b) $a = 51, b = 36$.

(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.