HOMEWORK 5

CS 191 - Discrete structures

Deadline: May 2 @ 23:55

There are *2* questions in this homework assignment. To get *any* credit, you must show *all* steps. A correct answer without steps will earn you 0 points.

Problem 1. Consider the integers 3213 and 1386.

- Find the gcd of 3213 and 1386 using the Euclidean algorithm.
- Find the gcd of 3213 and 1386 and express the gcd as a combination of these two integers using the **extended** Euclidean algorithm.

A *field* consists of a set S and two binary operations (functions) $+ : S \times S \to S$ and $\cdot : S \times S \to S$ called addition and multiplication, respectively. These data are required to satisfy some additional properties. The exact definition of fields is not important for this assignment. All you need to know is that there are distinguished elements $z \in S$ and $i \in S$ called the *additive identity* and the *multiplicative identity*, respectively. And for any element $n \in S$, with $n \neq z$, there is an element $n^{-1} \in S$, called the *multiplicative inverse for* n, such that $n \cdot n^{-1} = i$.

The set of real numbers $\mathbb{R}$ together with the usual addition and multiplication of real numbers form a field. The set of rational numbers $\mathbb{Q}$ together with their usual addition and multiplication also form a field. In fact, the set of Boolean values $\mathbb{B}$ can be equipped with a field structure: the xor function and the and function are the addition and multiplication, respectively.

A particular class of examples of fields consists of fields of the form $\mathbb{Z}_p$, where p is an arbitrary prime number. For a prime number p, the field $\mathbb{Z}_p$ consists of exactly p elements. Here is one way to construct such a field: recall that the congruence-modulo relation is an equivalence relation. Thus, we may take the set of equivalence classes of this equivalence relation as the underlying set of $\mathbb{Z}_p$. Addition and multiplication are given by $[n] +' [m] = [n + m]$ and $[n] \cdot' [m] = [n \cdot m]$, respectively. Here, $+$ and $\cdot$ are the usual additional and multiplication on integers, and $[n]$ is the equivalence class $\{ m \in \mathbb{Z} \mid n \equiv m \mod p \}$.

The multiplicative inverse for an element $[a]$, where $[a]$ is not the additive identity $[0]$, of the field $\mathbb{Z}_p$ is an element $[x]$ such that $[a] \cdot' [x] = [a \cdot x] = [1]$. To calculate this element, it suffices to find an integer x such that

$$a \cdot x \equiv 1 \mod p$$

Then the equivalence class represented by x is the desired multiplicative inverse. By unfolding the definition of congruence-modulo, this is equivalent to solving for x and y in the following equation:

$$ax + py = 1$$

Note that $\gcd(a, p)$ is necessarily 1 because p is a prime number. Then the problem reduces to finding a way to express 1 (the gcd) as a combination of a and p. By Bézout's lemma, this is always possible, and it can be computed via the extended Euclidean algorithm.

Problem 2. Use the extended Euclidean algorithm to find two integers x and y satisfying the following equation:

$$5x + 13y = 1$$

The equivalence class of x that you just computed is the multiplicative inverse for the element $[5]$ in the field $\mathbb{Z}_{13}$.