Homework #1. Due Wednesday, January 22nd, in class

Reading:

1. For this homework assignment: Chapter 1 and Section 2.1.
2. Before the class on Wed, Jan 22: Section 2.2-2.4.

Problems:

Problem 1: The Fibonacci numbers $f_1, f_2, \ldots$ are defined recursively by $f_1 = f_2 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. Prove that f_n and f_{n+1} are coprime for all n. (Two integers are called *coprime* if their greatest common divisor is equal to 1).

Problem 2:

(a) Let $d = gcd(123, 321)$. Find d and also find integers u and v such that $d = 123u + 321v$.

(b) Now find all integer pairs (x, y) such that $123x + 321y = 12$.

Problem 3: Let a and b be positive integers and $d = gcd(a, b)$.

(a) Prove that for any integer c such that $c > ab - a - b$ and $d \mid c$ there exist nonnegative integers x and y such that $c = ax + by$. **Hint:** Let x be the smallest nonnegative integer such that $c = ax + by$ for some $y \in \mathbb{Z}$ (explain why such x exists). Show that $x < b$ and deduce that y corresponding to this x is nonnegative.

(b) Assume that a and b are coprime, that is, $d = 1$. Prove that $c = ab - a - b$ cannot be written as $c = ax + by$ where x and y are nonnegative integers.

(c) Now assume that a and b are NOT coprime. Prove that $c = ab - a - b$ can be written as $c = ax + by$ for nonnegative integers x and y.

Problem 4: Let $n, m \in \mathbb{Z}$ and suppose that $gcd(n, m) = 1$. Prove that $gcd(n - m, n + m) = 1$ or 2 and show by examples that both possibilities may occur. **Hint:** Use Corollary 1.11(b) to prove that $gcd(n - m, n + m)$ divides 2.

Problem 5: Let G be a finite group and $g \in G$. Recall that the order of g, denoted by $o(g)$, is the smallest positive integer n such that $g^n = e$. Take any $m \in \mathbb{Z}$. Prove that $g^m = e \iff n \mid m$. **Hint:** For the forward direction use division with remainder.

Problem 6: The goal of this problem is to prove the 'yes' part of Problem 2 from Lecture 1: if $p \equiv 1 \mod 4$, then there exists $x \in \mathbb{Z}$ such that $p \mid (x^2+1)$. As explained in class, this is equivalent to proving that there exists $z \in \mathbb{Z}_p$ such that $z^2 + 1 = 0$ (where equality holds in $\mathbb{Z}_p$). You may use the following fact without proof:

Fact A: *The group* $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ *(with respect to multiplication) is cyclic.*

We will prove Fact A later in the course.

In all parts below, n is a positive integer, G is a cyclic group of order n and g is a generator of G.

(a) Prove that for every $d > 0$ which divides n, there exists $g_d \in G$ such that $o(g_d) = d$ and describe such g_d explicitly in terms of g, n and d (note that in general g_d is not unique).

(b) Now assume that n is even. Prove that G contains a unique element of order 2.

(c) Now let p be an odd prime, $n = p - 1$ and $G = \mathbb{Z}_p^\times$. What is the element of order 2 in G?

(d) Let p, n and G be as in part (c), and assume in addition that $p \equiv 1 \mod 4$. Use (a), (b) and (c) to show that there exists $z \in G$ such that $z^2 = -1$.