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).

Solution: We argue by induction. The base case $n = 1$ is clear.

Suppose now that $gcd(f_n, f_{n+1}) = 1$ for some $n \geq 1$. Then by Lemma 1.5 from the book $gcd(f_n + f_{n+1}, f_{n+1}) = gcd(f_n, f_{n+1}) = 1$. Since $f_n + f_{n+1} = f_{n+2}$, this finishes the induction step.

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 $123x + 321y = 12$.

Solution: (a) Using the Euclidean algorithm, we find that $d = 3$ and $3 = 123 \cdot 47 + 321 \cdot (-18)$. If you forgot how to apply the Euclidean algorithm, you can review it, for instance, in Lecture 4 of the Survey of Algebra notes.

(b) Multiplying both sides of $123 \cdot 47 + 321 \cdot (-18) = 3$ by 4, we get $123 \cdot 188 + 321 \cdot (-72) = 12$, so $(x_0, y_0) = (188, -72)$ is a particular solution. By Theorem 1.13 (from the book), the general solution is $x = 188 + \frac{321}{3}k = 188 + 107k$, $y = -72 - \frac{123}{3}k = -72 - 41k$ with $k \in \mathbb{Z}$.

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.

Solution: Throughout the argument by a solution to $ax + by = c$ we will always mean an integer solution.

(a) Since $d \mid c$, the equation does have a solution; moreover, by Theorem 1.13 the x-components of the set of all solutions form an arithmetic progression (infinite in both directions), so there is a solution (x, y) with $x \geq 0$. By the well-ordering principle, there is a solution (x_0, y_0) with $x_0 \geq 0$ and x_0 smallest possible. Note that $(x_0 - b, y_0 + a)$ is also a solution (either by direct verification or using the formula for the general solution). Since $x_0 - b < x_0$, by the choice of x_0 we must have $x_0 - b < 0$, whence $x_0 - b \leq -1$ (since $x_0 - b \in \mathbb{Z}$) and hence $x_0 \leq b - 1$. Then $ax_0 \leq a(b-1) = ab - a$ and $ax_0 + by_0 \leq ab - a + by_0$. But $ax_0 + by_0 = c > ab - a - b$ by assumption, so $ab - a + by_0 > ab - a - b$ and $by_0 > -b$. Dividing both sides by b, we get $y_0 > -1$, and since $y_0 \in \mathbb{Z}$, we conclude that $y_0 \geq 0$. Thus, (x_0, y_0) is a non-negative integer solution.

(b) By direct verification $(x_0, y_0) = (-1, a-1)$ is a solution. Since $d = 1$, the general solution is $x = -1 + bk$, $y = a - 1 - ak$. But $-1 + bk \leq 0$ for all $k \leq 0$ while $a - 1 - ak \leq 0$ for all $k \geq 1$, so there is no integer k for which both $x = -1 + bk$ and $y = a - 1 - ak$ are non-negative.

(c) As in (b) $(x_0, y_0) = (-1, a-1)$ is a solution, whence $(x, y) = (-1 + \frac{b}{d}, a - 1 - \frac{a}{d})$ is also a solution. Note that $-1 + \frac{b}{d} \geq 0$ since $\frac{b}{d}$ is a positive integer. Also by assumption $d \geq 2$, so $a - 1 - \frac{a}{d} \geq a - 1 - \frac{a}{2} = \frac{a}{2} - 1 \geq 0$ (since $\frac{a}{d}$ is a positive integer). Thus, (x, y) is a non-negative integer solution.

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.

Solution: We will show that $gcd(n - m, n + m)$ divides 2 following the hint, but the suggestion to use Corollary 1.11(b) was misleading.

Let $d = gcd(n - m, n + m)$. Then $d \mid (n - m)$ and $d \mid (n + m)$, so $d \mid (n - m) + (n + m) = 2n$ and $d \mid (n + m) - (n - m) = 2m$. By the properties of the greatest common divisor, since $d \mid 2n$ and $d \mid 2m$, we must have $d \mid gcd(2n, 2m)$. But by Corollary 1.10 from the book $gcd(2n, 2m) = 2gcd(n, m) = 2$, so $d \mid 2$ and hence $d = 1$ or 2 (since by definition $d > 0$).

If $n = 2$ and $m = 1$, then $gcd(n, m) = 1$ and $gcd(n - m, n + m) = 1$, and if $n = 3$ and $m = 1$, then $gcd(n, m) = 1$ and $gcd(n - m, n + m) = 2$, so both possibilities may occur.

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 $g^m = e \iff o(g) \mid m$.

Solution: Let $n = o(g)$, and divide m by n with remainder: $m = nq + r$ with $0 \leq r < n$. Then $g^m = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r$, so $g^m = e \iff g^r = e$. Since $0 \leq r < n = o(g)$, we have $g^r = e \iff r = 0$. Hence $g^m = e \iff r = 0 \iff n \mid m$.

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 $z^2 = -1$.

Solution: (a) Let $g_d = g^{n/d}$. Then $g_d^d = g^n = e$. Also if $0 < k < d$, then $0 < \frac{n}{d}k < n$, so $g_d^k = g^{\frac{n}{d}k} \neq e$, so g_d^d is the smallest positive power of g_d equal to e. Hence by definition of the order $o(g_d) = d$.

(b) By (a) the element $g^{\frac{n}{2}}$ has order 2. Now let h be any element of G of order 2. Since g is a generator of G and $n = |G|$, we can write $h = g^m$ for

some $0 < m < n$ (we cannot have $m = 0$ since otherwise $h = e$ has order 1). Then $e = h^2 = g^{2m}$, so by part (a) we must have $n \mid 2m$. But $0 < m < n$, so $0 < 2m < 2n$, and the only multiple of n strictly between 0 and $2n$ is n. Hence $2m = n$, so $m = \frac{n}{2}$ and $h = g^{\frac{n}{2}}$. So $g^{\frac{n}{2}}$ is the unique element of order 2 in G.

(c) $[-1]$ is clearly an element of order 2 (and by part (b) it is the unique element of order 2)

(d) Since $p \equiv 1 \mod 4$, the order of G is divisible by 4, so by (a) there exists $z \in G$ which has order 4. Then $z^2 \neq [1]$, but $(z^2)^2 = z^4 = [1]$, so z^2 is an element of order 2. By (c), we must have $z^2 = [-1]$.