Homework 1

MATH 301/601
Test #1 is on Tuesday, February 18

Instructions. *Read the Homework Guide to make sure you understand how to successfully complete the assignment.*

***Exercise 1.** (a) Give an example of a function $\mathbb{N} \to \mathbb{N}$ that is injective but not surjective.

(b) Give an example of a function $\mathbb{N} \to \mathbb{N}$ that is surjective but not injective.

(c) Give an example of a bijection from $\mathbb{N} \to \mathbb{Z}$.

Exercise 2. Let $f\colon A \to B$ and $g\colon B \to C$. Prove the following statements.

(a) If f and g are both injective, then $g \circ f$ is injective.

(b) If $g \circ f$ is surjective, then g is surjective.

(c) If $g \circ f$ is injective and f is onto, then g is injective.

Exercise 3. Let $f\colon X \to Y$ be a function, let $A_1, A_2 \subset X$, and let $B_1, B_2 \subset Y$.

(a) Prove that $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Prove that $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$, and then give an example where $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$.

(c) Prove that $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, where $f^{-1}(B) = \{x \in X : f(x) \in B\}$.

(d) Prove that $f^{-1}(B_1 \cap B_2) = f^{-1}(B_2) \cap f^{-1}(B_2)$.

***Exercise 4.** Let $S \subset \mathbb{N}$ such that $1 \in S$ and $n + 1 \in S$ whenever $n \in S$. Prove that $S = \mathbb{N}$. (Hint: Use the well-ordering principle.)

****Exercise 5.** Define the ordering $<$ on $\mathbb{N} \times \mathbb{N}$ by $(a, b) < (c, d)$ if $a < c$ or $a = c$ and $b < d$ (this is called the *lexicographical ordering*). Prove that $(\mathbb{N} \times \mathbb{N}, <)$ is well ordered, that is, show that given a nonempty subset S of $\mathbb{N} \times \mathbb{N}$ there exists $s \in S$ such that $s < s'$ for all $s' \in S \smallsetminus \{s\}$.
Aside: as a set with no additional structure, $\mathbb{N} \times \mathbb{N}$ is equivalent to $\mathbb{N}$, as there is a bijection between them (can you find it?); however, as ordered sets, these sets are not equivalent (meaning, there is no order-preserving bijection between them), as bounded sets need not be finite in the lexicographical ordering. Various notions of equivalence are very important in mathematics.

Exercise 6. Let $a, b, c, m, n \in \mathbb{Z}$. Prove that if $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$.

Exercise 7. Let $a, b \in \mathbb{Z}$. Prove that if $a \mid b$ and $b \mid a$, then either $a = b$ or $a = -b$.

***Exercise 8.** Let $n \in \mathbb{N}$. Prove that the remainder obtained from dividing n^2 by 4 is either 0 or 1.

Exercise 9. Use the Euclidean algorithm to compute the following greatest common divisors:

(a) $\gcd(42, 55)$

(b) $\gcd(14, 30)$

(c) $\gcd(234, 165)$

(d) $\gcd(1739, 9923)$

***Exercise 10.** Let $a, b \in \mathbb{Z} \setminus \{0\}$. Prove that if there exists $s, t \in \mathbb{Z}$ such that $as + bt = 1$, then $\gcd(a, b) = 1$.

Exercise 11. Let a and b be nonzero integers, and let $d = \gcd(a, b)$. Prove that an integer c is a linear combination of a and b if and only if $d \mid c$.

Definition. Two nonzero integers are *relatively prime* if their greatest common divisor is one.

Exercise 12. Let a and b be relatively prime integers. Prove that if $c \in \mathbb{Z}$ such that $a \mid bc$, then $a \mid c$.

Exercise 13. Let $p \in \mathbb{N}$ be prime. Prove that if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that $p \mid a_1 a_2 \cdots a_n$, then there exists $k \in \{1, 2, \ldots, n\}$ such that $p \mid a_k$. (Hint: Use induction, with Euclid's lemma as the base case.)

Definition. Given two nonzero integers a and b, an integer c is a *common multiple* of a and b if $a \mid c$ and $b \mid c$. The *least common multiple* of a and b, denoted $\operatorname{lcm}(a, b)$, is the smallest positive common multiple of a and b.

***Exercise 14.** Let a and b be nonzero integers.

(1) Prove that the least common multiple of a and b exists.

(2) Prove that if $k \in \mathbb{Z}$ is a common multiple of a and b, then $\operatorname{lcm}(a, b)$ divides k. (Hint: divide k by $\operatorname{lcm}(a, b)$ using the division algorithm.)

****Exercise 15.** Let a and b be nonzero integers.

(1) Prove that the product of $\mathrm{lcm}(a, b)$ and $\gcd(a, b)$ is equal to $|ab|$. (Hint: the product ab is divisible by $d = \gcd(\mathrm{a}, \mathrm{b})$. Let $m = |ab|/d$. Now, let k be a common multiple of a and b. Write d as a linear combination in a and b, and use this to express the fraction k/m as an integer.)

(2) Prove that $\mathrm{lcm}(a, b) = |ab|$ if and only if $\gcd(a, b) = 1$.

Exercise 16. Let $a \in \mathbb{Z} \setminus \{1\}$. Use induction to prove that

$$a^n - 1 = (a - 1) \sum_{k=0}^{n-1} a^k$$

for all $n \in \mathbb{N}$. (Note: you are inducting on n, not a.)

***Exercise 17.** Let $p \in \mathbb{N}$ with $p \geq 2$. Prove that if $2^p - 1$ is prime, then p is prime. (Hint: you will find the previous exercise helpful.)