Math 4000/6000 – Homework #1

posted January 15, 2018; due at the **start of class** on January 24, 2018

> You know, for a mathematician, he did not have enough imagination. But he has become a poet and now he is fine.
> — David Hilbert (1862–1943), talking of an ex-student

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

For **problems #1 and #2 only**, you must explicitly justify each of your algebraic steps using our axioms for the integers (the properties listed on the handout). You may assume $-(-a) = a$ and $(-1)a = -a$, as these results were already discussed in class. For a model, look back at your notes for the proof done in class that $a \cdot 0 = 0$.

1. (Trichotomy for integer inequalities) Let $a, b \in \mathbb{Z}$.
   (a) Prove that $-(a + -b) = b + -a$.
   (b) Using the result of (a) and property O1, show that for any integers a, b exactly one of the following holds: $a < b$, $a = b$, or $a > b$. [1]

2. Prove that for any $a, b \in \mathbb{Z}$, we have
   (a) $(-a)b = -(ab)$,
   (b) $(-a)(-b) = ab$.

3. Let $a, b \in \mathbb{Z}$.
   (a) Prove that if $a < 0$ and $b < 0$, then $ab > 0$.
   (b) Show that if $a < 0$ and $b > 0$, then $ab < 0$.
   (c) Show that if $ab = 0$, then either $a = 0$ or $b = 0$.

   [In this problem and the rest, you can take *algebraic* properties of the integers for granted; for instance, you can assume things like $-(a - b) = -a + b$ and $-(-a)c = ac$. But you still need to justify your answers using our definition of inequalities along with the order properties of integers (O1 of the handout).]

4. Let S be a subset of the complex numbers. Show that it is impossible for S to have all of the following three properties:
   (i) the sum of two elements of S is always in S,
   (ii) the product of two elements of S is always in S,
   (iii) for each complex number x, exactly one of the following holds: $x = 0$, $x \in S$, or $-x \in S$.

[1] Recall that "$a < b$" means that $b + -a \in \mathbb{Z}^+$, while "$a > b$" means the same as "$b < a$". Also note that the book uses $\mathbb{N}$ for what we call $\mathbb{Z}^+$.

This proves that the complex numbers cannot be ordered! For this problem, you may use any familiar facts about the complex numbers and do not have to base your justifications on the handout.

5. (Laws of exponents) Let $a \in \mathbb{Z}$. Suppose that m, n belong to the set $\mathbb{Z}^+ \cup \{0\}$ of nonnegative integers.

   (a) Prove that $a^m \cdot a^n = a^{m+n}$.

   (b) Prove that $a^{mn} = (a^m)^n$.

   Hint: If $m = 0$ or $n = 0$, this is easy (why?). So you can suppose $m, n \in \mathbb{Z}^+$. Now think of m as fixed and proceed by induction on n.

6. Use the binomial theorem to find closed forms for the following sums, as functions of n, where n is assumed to be a natural number. (It might help to work out the sums for the first few natural numbers n.)

   (a) $\displaystyle\sum_{k=0}^{n} \binom{n}{k}$.

   (b) $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k}$.

7. In this exercise we outline a proof of the following statement, which was left as a "missing step" in our proof of the division theorem: If $a, b \in \mathbb{Z}$ with $b > 0$, the set

$$S = \{a - bq : q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$$

   has a least element.

   (a) Prove the claim in the case $0 \in S$.

   (b) Prove the claim in the case $0 \notin S$ and $a > 0$.

   (c) Prove the claim in the case $0 \notin S$ and $a \leq 0$.

   Hint: (a) is easy. To handle (b) and (c), first show that in these cases S is a nonempty set of natural numbers, so that the well-ordering principle guarantees S has a least element as long as S is nonempty. To prove S is nonempty, show that in case (b), the integer a is an element of S. You will have to work a little harder to prove S is nonempty in case (c).

8. Use the Euclidean algorithm to find $\gcd(314, 159)$ and $\gcd(272, 1479)$. Show the steps, not just the final answer.

9. Show that if $a, b \in \mathbb{Z}^+$ and $a \mid b$, then $a \leq b$.

10. Let a, b be nonnegative integers, not both zero. Define the set

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

   (Thus, $I(a, b)$ is the set of all linear combinations of a, b, with coefficients from $\mathbb{Z}$. The letter I stands for *ideal*, which is a concept we will meet later in the course.)

(a) Show that if a, b, q, r are integers with $a = bq + r$, then $I(a, b) = I(b, r)$.

(b) Explain why (a) implies that $I(a, b) = I(0, \gcd(a, b))$.

(c) Deduce from (b) that there are integers x and y with $\gcd(a, b) = ax + by$.

11. (*) Exercise 1.1.16 (this means Exercise 16 in §1 of Chapter 1)

    Hint: The *odd part* of a positive integer n is its largest odd divisor. For example, the odd part of 25 is 25, while the odd part of 212 is 53. First show that among any $n+1$ numbers in the set $\{1, 2, 3, \ldots, 2n\}$, two have the same odd part.