A biologist, a physicist and a mathematician were sitting in a street cafe watching the crowd. Across the street they saw a man and a woman entering a building. Ten minutes they reappeared together with a third person.
– They have multiplied, said the biologist.
– Oh no, an error in measurement, the physicist sighed.
– If exactly one person enters the building now, it will be empty again, the mathematician concluded.

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. Fully explain your answers. In problems #1(a) and #2 only, you must justify which algebraic properties (properties A1–A4, M1–M3, D1 on the handout) you are using at every step of the proof. In your write-up, please refer to these properties by name rather than number. You may assume that $a \cdot 0 = 0$ and $(-1)a = -a$ for all $a$, as already shown in class. For all other problems, you do not have to justify those kinds of algebraic manipulations. Note: $\mathbb{Z}^+$ means the same as $\mathbb{N}$ (the book’s notation).

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

2. Let $a, b \in \mathbb{Z}$ and suppose that $a < b$.
   (a) Prove that $a + c < b + c$ for every $c \in \mathbb{Z}$.
   (b) Prove that $ac < bc$ for every $c \in \mathbb{Z}^+$.

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 $b = 0$.

4. (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 $n$.

5. In this exercise we outline a proof of the following statement, which we will be taking for granted 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).

6. Use the binomial theorem to find formulas for the following sums, as functions of $n$, where $n$ is assumed to be a natural number.

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

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

7. (To be done after Monday’s lecture) Use the Euclidean algorithm to find $\gcd(314, 159)$ and $\gcd(272, 1479)$. Show the steps, not just the final answer.

8. Show that if $a, b \in \mathbb{N}$ and $a \mid b$, then $a \leq b$.

9. 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 $\gcd(a, b) = ax + by$.

10. (*) We stated the binomial theorem under the assumption that $x, y \in \mathbb{Z}$. However, our proof only used that we could manipulate expressions in $x$ and $y$ by the usual algebraic rules. That assumption holds if $x, y$ are formal symbols manipulated according to the usual rules for polynomials. Hence, the identity

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

is valid as a polynomial identity in the variables $x$ and $y$. (So far I have not asked you to prove anything, just to accept this as true!)

Your mission: By computing $(x + y)^{2n}$ in two different ways and comparing coefficients, show that for every positive integer $n$,

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$ 

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

Hint: Start by writing each number in $\{1, 2, \ldots, 2n\}$ in the form $2^j \cdot q$, where $j$ is a nonnegative integer and $q$ is odd.