CAAP Math C, Mr. Church, Final Exam
Wednesday, August 13
`http://www.math.uchicago.edu/~tchurch/`

Write your name on the front of your test book. **You should write all answers in the blue book provided. Do not write your answers on this sheet.** Please label your answers clearly in your test book. You have 90 minutes to complete this test. There are 175 points available, but the test will be graded as if it were out of 150 points.

On the last page of the exam, there is a sheet listing the axioms that we have discussed and a few definitions. You should refer to it during the test, especially on questions 1 and 5.

The five questions are roughly ordered from easier to harder; harder questions are worth more points. Every section of every question is independent of the other sections, except 1(c) which relies on 1(a). You may skip around and answer any sections you can, in any order, as long as your answers are clearly labeled.

1. (20 points) Note that neither 91 nor 65 is prime.
   (a) (5 points) Compute $\gcd(91, 65)$ using the Euclidean algorithm.
   (b) (5 points) Compute $\gcd(91, 65)$ using prime factorizations.
   (c) (10 points) Use the Euclidean algorithm to find integers x and y so that you can write $\gcd(91, 65) = 91x + 65y$.

2. (20 points) Let $f\colon A \to B$ be a function from the set A to the set B.
   (a) (10 points) Prove that if there exists a function $g\colon B \to A$ such that $g \circ f\colon A \to A$ satisfies $g \circ f(a) = a$ for all $a \in A$, then f is one-to-one.
   (b) (10 points) Prove that if there exists a function $h\colon B \to A$ such that $f \circ h\colon B \to B$ satisfies $f \circ h(b) = b$ for all $b \in B$, then f is onto.

3. (30 points) Let $(R, +, *)$ be a commutative ring (that is, Axioms A1–A4, M1–M3, and D all hold). Let $0 \in R$ be the additive identity. Prove from the axioms mentioned above that $0 * r = r * 0 = 0$ for any $r \in R$; at each step, say which axioms you are using.

4. (30 points) Let $\mathcal{M}_2 = \{n \in \mathbb{Z} | n \equiv 0 \pmod 2\}$ be the set of even integers, let $\mathcal{M}_3 = \{n \in \mathbb{Z} | n \equiv 0 \pmod 3\}$ be the set of multiples of three, and let $\mathcal{M}_6 = \{n \in \mathbb{Z} | n \equiv 0 \pmod 6\}$ be the set of multiples of 6.
   (a) (15 points) Prove that $(\mathcal{M}_2 \cap \mathcal{M}_3) \subseteq \mathcal{M}_6$.
   (b) (15 points) Prove that $\mathcal{M}_6 \subseteq (\mathcal{M}_2 \cap \mathcal{M}_3)$.

   It follows that $\mathcal{M}_2 \cap \mathcal{M}_3 = \mathcal{M}_6$.

5. (75 points) Recall that $\mathbb{Z} \times \mathbb{Z}$ is defined to be the set of pairs (n, m) where n and m are both integers. We define three operations on $\mathbb{Z} \times \mathbb{Z}$:

$$
\begin{aligned}
(a, b) + (c, d) &= (a + c, b + d) \\
(a, b) \bullet (c, d) &= (ac, bd) \\
(a, b) \star (c, d) &= (ac - bd, bc + ad)
\end{aligned}
$$

(a) (10 points) Show that the operation $\star$ is associative, meaning that

$$\Big((a, b) \star (c, d)\Big) \star (e, f) = (a, b) \star \Big((c, d) \star (e, f)\Big)$$

for all integers a, b, c, d, e, and f.

In fact, $(\mathbb{Z} \times \mathbb{Z}, +, \star)$ satisfies Axioms A1–A4, M1–M3, and D, and is thus a commutative ring. $(\mathbb{Z} \times \mathbb{Z}, +, \bullet)$ also satisfies these axioms, and is thus also a commutative ring.

(b) (5 points) Show that $(0, 0)$ is the identity for the operation $+$.

(c) (5 points) What is the identity for the operation $\bullet$?

(d) (5 points) What is the identity for the operation $\star$?

(e) (15 points) Give an example of a zero-divisor (a, b) in the commutative ring $(\mathbb{Z} \times \mathbb{Z}, +, \bullet)$, and show that it is a zero-divisor; that is, find some $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ such that $(a, b) \bullet (c, d) = (0, 0)$ but $(c, d) \neq (0, 0)$.

(f) (10 points) Prove that if $(a, b) \star (a, b) = (0, 0)$, then $a = 0$ and $b = 0$.

For the next two questions, just the answer "Yes" or "No" is worth no points, even if it is correct. You must justify your answer (how to justify it is written below).

(g) (10 points) Does there exist a square root of $(-1, 0)$ with respect to the operation $\star$? That is, is there some (a, b) such that $(a, b) \star (a, b) = (-1, 0)$? If so, find all such square roots; if not, prove none exists.

(h) (10 points) Does there exist a square root of $(-1, 0)$ with respect to the operation $\bullet$? That is, is there some (a, b) such that $(a, b) \bullet (a, b) = (-1, 0)$? If so, find all such square roots; if not, prove none exists.

There is no homework due Monday. Have a good weekend!