Exam 3 **Name:** _____

MTH182, Section 03 April 9, 2015

This test is:

- closed-book
- closed-notes
- no-calculator
- 75 minutes

Indicate your answers clearly, and show your work. Partial credit will be awarded based on work shown. Full credit will not be awarded without some work shown.

Fun fact of life: if your work is not legible, I will not be able to read it. The ramifications of this outcome should be clear.

There are four questions, some with multiple parts; each question is worth a total of 25 points.

All pages are one-sided. If on any problem you require more space, use the back of the page.

DO NOT TURN THIS PAGE UNTIL DIRECTED TO BEGIN

1. (25 pts total) This question concerns divisibility.

a.) (5 pts) Determine whether $3 \mid 6$. Justify your answer.

b.) (5 pts) Determine whether $-2 \mid 2$. Justify your answer.

c.) (5 pts) Determine whether $1 \mid 10$. Justify your answer.

d.) (5 pts) If $a \mid b$ and $b \mid a$, does it follow that $a = b$? Why or why not?

e.) (5 pts) Let a and b be integers. Suppose $a \mid b$. Does it follow that $(-a) \mid b$? Prove or disprove.

2. (25 pts total) This question concerns the division algorithm.

a.) (5 pts) Compute $5 \bmod 2$, and $5 \operatorname{div} 2$.

b.) (5 pts) Compute $-12 \bmod 7$, and $-12 \operatorname{div} 7$.

c.) (5 pts) Compute $23 \bmod 24$, and $23 \operatorname{div} 24$.

d.) (10 pts) Let a, b, and c be any three *consecutive* integers. Use the division algorithm to prove that 3 divides one of these three integers.

3. (25 pts total) This question concerns modular congruence of integers.

a.) (5 pts) Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. *Define* what $a \equiv b (\bmod n)$ means. (I will accept any one of several "definitions" that was discussed in class and in the book.)

b.) (5 pts) Is $-3 \equiv 7 (\bmod 4)$?

c.) (5 pts) Is $3 \equiv -17 (\bmod 5)$?

d.) (10 pts) Let $a \equiv 0 (\bmod 3)$, and $b \equiv 2 (\bmod 3)$. Prove that $a^2 + b^2 \equiv 1 (\bmod 3)$.

4. (25 pts total) This question concerns cryptographic ciphers that interpret letters A, B, ..., Z as the integers $0, 1, \ldots, 25$. Consult the cipher sheet provided with this exam.

In this question, answers must be provided as alphabetical characters, not integers.

a.) (10 pts total) Encrypt the message "TIMSHEL" using the encryption function $f(x) = (x + 4) \bmod 26$.

b.) (5 pts total) Suppose an encryption function is defined as $f(x) = (2x) \bmod 26$. Why is this a bad choice of encryption function?

c.) (10 pts total) An encrypted message reads "URVHEXG", and was encrypted using the encyrption function $f(x) = (x + 3) \bmod 26$. What is the original (decrypted) message?