## Math 126, first test sample problems.

These are sample questions. You may bring one sheet of prepared notes for the test. Calculators are optional; you may bring one if you like.

Problem 1. Carefully prove the following statement. If $p$ is a prime, and $n$ any positive integer, then the greatest common divisor $(p, n)$ is either 1 or $p$.

Problem 2. On the Euclidean algorithm.
a. Apply the Euclidean algorithm to show that the greatest common divisor of 1001 and 805 is 7 .
b. Use the results of the computation in part a to express 7 as a linear combination of 1004 and 805.
c. For each of the following two linear Diophantine equations, either find a solution, or explain why no solution exists.

$$
\begin{array}{r}
1001 x+805 y=14 \\
1001 x+805 y=3
\end{array}
$$

Problem 3. On divisors.
a. Draw the Hasse diagram of the divisors of 200 .
b. What are the values of $d(200)$ and $\sigma(200)$.
c. Is the number 200 a perfect number? Why or why not?

Problem 4. Since 19 is a prime number, $\mathbf{Z}_{19}$ is a field, and division, except by 0 , works in $\mathbf{Z}_{19}$. Thus, there is some $x$ such that

$$
6 x \equiv 1(\bmod 19)
$$

Find such an $x$. In one sentence, explain the method you used to find the solution.
Problem 5. Prove that if $a \equiv b(\bmod n)$, and $c \equiv d(\bmod n)$, then $a-c \equiv b-d(\bmod n)$.
Problem 6. True or false. Just write the word "true" or the word "false". If it's not clear to you which it is, explain; otherwise no explanation is necessary.
a. The principle of mathematical induction is used to make conjectures about numbers, but it sometimes makes wrong conclusions.
b. If $a, b$, and $c$ are integers, then $(a, b)=(a-c b, b)$.
c. If an integer $n$ is not a perfect cube (i.e., not the cube of any integer), then the cube root $\sqrt[3]{n}$ is an irrational number.
d. Although Euclid devoted three of the books of his Elements to number theory, he stated no axioms for numbers.
e. A Pythagorean triple consists of three positive integers $a, b$, and $c$ such that $a^{2}+b^{2}=c^{2}$.

