Practice for Final Exam, part 1 — Test is 2 July 2004

Math 2770

30 June 2004

Dr. Michael Oliver

1) Let $a, c, d \in \mathbb{Z}$, and suppose $a|d$, $c|d$, but $a \nmid c$ (this last is to be read "a does *not* divide c"). Does a divide $7c + 2d$? Choose one of the following and follow the instructions:

a) Yes, always (you must prove it)

b) No, never (you must prove it)

c) Sometimes yes and sometimes no (you must find values of a, c, d, satisfying the conditions, for which the answer is "yes", and other values for which the answer is "no").

2) Let $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$ be some given functions. Suppose Alice and Bob play the following game:

Alice				$n =$
Bob	$M =$	$C_1 =$	$C_2 =$	

The rules are: Alice and Bob must play natural numbers. Bob wins if $n \leq M$ or $\frac{g(n)}{C_1} \leq f(n) \leq C_2 \cdot g(n)$; otherwise, Alice wins.

a) Write a sentence of quantified first-order logic that is true (interpreted with the natural numbers as the universe of discourse) if and only if Bob has a winning strategy for the game.

b) Explain what the above sentence "says", in terms of notation we've used in class.

3) Let A, B, and C be sets (and suppose that they are all subsets of some fixed universal set). Find another form for the expression $\overline{A \cup (B \setminus C)}$. In your new form, no overline should appear over more than one letter at a time.

4) Suppose $f : A \to B$ and $g : B \to C$ are 1-1. Is $(g \circ f) : A \to C$ necessarily 1-1? Prove your answer.

5)

a) Does 17 have a multiplicative inverse modulo 48? If so, what is it? If not, why not? (Hint: Euclid's Algorithm may be useful, whether the answer is yes or no.)

b) Suppose someone knows a number M, with M between 0 and 105 and relatively prime to 105. Suppose this person sends you a number $C = M^{17} \pmod{105}$. Can you determine the value of M in an efficient manner (say, not by trying every possibility)? Explain.

6) Prove or refute: For any natural numbers n and m and any k such that $n|k$ and $m|k$, it follows that $\text{lcm}(n, m)|k$. You may use either the Fundamental Theorem of Arithmetic or the fact that $\gcd(n, m) \cdot \text{lcm}(n, m) = nm$.