# MATH 471 FINAL EXAM

This exam is worth 140 points, with each problem worth 20 points. Please complete Problem 1 and then *any six* of the remaining problems. *There are problems on both sides.* Unless indicated, you must justify your answer to receive credit for a solution.

When submitting your exam, please indicate which problems you want graded by writing them in the upper right corner on the cover of your exam booklet. You must select exactly four problems; any unselected problems will not be graded, and if you select more than four only the first four (in numerical order) will be graded.

(1) Please classify the following statements as *True* or *False*. Write out the word completely; do not simply write $T$ or $F$. There is no partial credit for this problem, and it is not necessary to show your work for this problem.

Note that for a statement to be *True*, it must be true *exactly as written and for all cases*. To be *False*, there needs to be only one example showing that the statement is false. A statement that is "true most of the time, except sometimes" is false in mathematics.

(a) The Euler phi function satisfies $\varphi(a)\varphi(b) = \varphi(ab)$ for all positive integers $a, b$.
(b) In an *asymmetric* cryptographic system, it is difficult to compute how to decrypt messages from the knowledge of the encrypting function.
(c) The greatest common divisor satisfies $(a, b) = (a + b, b)$ for all positive integers $a, b$.
(d) There are exactly six integers $n$ such that $12 \mid n$ and $n \mid 816$.
(e) If $f, g$ are arithmetic functions with $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} f(d/n)$.

(2) A magic word is encrypted using the RSA method. The published public key data is $(e, N) = (107, 187)$. The encrypted magic word is

```
060 165 000 171 178 002 161 171
```

Can you decrypt the message?

(3) A group of friends wants to play cards. Unfortunately their card deck is missing many of its 52 cards. They try to deal out poker hands (5 cards each), and discover they have 4 cards left over. They try to deal out rummy hands (7 cards each), and again have 4 cards left over. Finally they try to play war, which requires the deck to be dealt out evenly between two teams, and they discover after dealing that they have one card left over. Can you determine how many cards they have from this information?

(4) (a) Define the Möbius function $\mu(n)$.
(b) Prove that $\mu(n)$ is multiplicative.
(c) Is $\mu(n)$ completely multiplicative?
(d) The *Mertens functon* is defined by $M(n) = \sum_{i=1}^{n} \mu(i)$. Compute $M(30)$.

---

*Date*: Monday, 15 December 2008.

(5) Use Hensel's lemma to find the roots of the polynomial $f(x) = x^3 + x^2 + 1$ modulo $3, 3^2, 3^3, 3^4$.

(6) (a) Compute the greatest common divisor $d$ of 10 and 13, and represent $d$ as an integral linear combination of these numbers.
    (b) Find three positive integers such the GCD of any two of them is larger than 1, yet the GCD of all three equals 1.
    (c) Let $n > 3$ be an integer. Explain how to find $n$ positive integers such that any subset of size $\leq n - 1$ has GCD $> 1$, yet the GCD of all $n$ is 1.

(7) (a) Show that 6601 is a 5-pseudoprime.
    (b) Is 6601 a strong 5-pseudoprime?

(8) (a) Compute $\varphi(10^n)$, $n = 1, 2, 3, \ldots$
    (b) Find all positive integers $n$ such that $\varphi(n) = 20$.

(9) Factor 8633 using
    (a) Fermat factorization
    (b) Pollard $\rho$ factorization
    (c) Pollard $p - 1$ factorization

(10) Show that if $m, n$ are positive integers with $(m, n) = p$, where $p$ is a prime, then $\varphi(mn) = p\varphi(m)\varphi(n)/(p - 1)$.