MTH 211: End-semester exam

Maximum marks: 100 **Time:** 3 hours

Instructions. Be sure to show your work and explain your reasoning for full credit. No calculators, phones, notes, etc. are allowed. Please write your answers in the sequence of questions asked (**-2 points** for not following this rule).

1. ((4×7) points) The following are **true/false** questions. If you think the statement is true, give a proof, stating any theorems you need. If false, provide a concrete counterexample or give a proof.

   (a) The quadratic congruence $x^2 \equiv a \pmod{2}$ is solvable for all a, except $a \equiv 1 \pmod{4}$.

   (b) The quadratic congruence $x^2 \equiv a \pmod{4}$ is solvable for all $a \equiv 1 \pmod{4}$.

   (c) An integer n is composite if and only if n does not divide $(n-1)!+1$.

   (d) The numbers $0, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ form a complete system of residue modulo 7.

   (e) There exists an integer x such that $3x \equiv 347 \pmod{453}$.

   (f) The divisor function is multiplicative.

   (g) The Euler phi function is completely multiplicative.

2. ((5×3) points) The following problems test your knowledge of theorems and definitions: State the theorem or definition requested; be sure to include any necessary hypotheses, and details.

   (a) State one primality test covered in class.

   (b) What is a pseudo-prime to base 11? What is a Carmichael number?

   (c) State Wilson's theorem.

3. ((6×4) points) Each of the following questions can be answered using only a minimal amount of pencil/paper calculations if *approached with the right method.* If you get stuck in a messy hand computation, you are on the wrong track. Answers arrived at by brute force methods, trial and error, or guessing won't earn credits.

   (a) Find the last two decimal digits of 413^{402}.

   (b) Find the general solution to the equation $13x + 11y = 7$.

   (c) Find the value of the Legendre symbol $\left(\frac{-461}{383}\right)$. (Show all work, for the key steps, indicate which rule or property of the Legendre symbol you are using. 383 is prime.)

   (d) Find inverse of 5 mod 26.

4. ((6×5) points) Short proofs.

   (a) In the RSA encryption system, a message M is encrypted by computing $E \equiv M^e \pmod{m}$, where e is the public encryption exponent and m the public modulus. The encrypted message E is decrypted by computing $E^d \pmod{m}$, where d is the decryption exponent. State precisely how d is defined, and prove that with this choice of d decryption returns the original message M, i.e., $E^d \equiv M \pmod{m}$.

   (b) Prove that p is a prime greater than 3, then at least one of $p+2$ and $p+4$ are composite.

   (c) Prove that if $n = a^2 + b^2$ for some $a, b \in \mathbb{Q}$, then $n = c^2 + d^2$ for some $c, d \in \mathbb{Z}$.

   (d) Prove that 561 is a Pseudoprime.

   (e) Use Euler's theorem to prove $n^7 \equiv n \pmod{63}$ for all positive integers n with $(n, 3) = 1$.

5. (5 points) Find the number α with the continued fraction expansion $[1, 2, 3, 2, 3, \cdots]$.

6. (Bonus question, 5 points) What was your favorite topic, and why?