MATH 312 FINAL EXAM

DECEMBER 10, 2014

Name: ____

Student number: ____

Instructions

This exam has **7 problems**. Point values are noted before each problem.

- Problem 1 is a True/False problem for which you do not need to show any work. More instructions are given in the problem statement.

- For Problems 2, 3, and 4, you should clearly write out the steps of your calculations, but you do not need to cite any theorems you use.

- For Problems 5, 6, and 7, you should write clear and complete proofs. If your proof uses a theorem we've proved in class or in the text, then give a brief statement or paraphrase of that theorem.

There are **100 points total**.

Academic Integrity

No calculators, books, or notes are allowed. The only items you may have on your desk are a pen or pencil, eraser, and ID card. It is a serious offense to use unauthorized notes or to exchange information with another student during the exam.

Problem 1: 12 parts, 24 pts total

Mark each of the following twelve statements TRUE or FALSE. Mark a statement as TRUE if and only if it is *true for all possible values of the unknowns*; otherwise, mark it as FALSE. Each part is worth 2 points. You do not have to show any work, and no partial credit will be given.

(1a) There are exactly 12 primitive roots (mod 29) in any reduced residue system (mod 29).

TRUE FALSE

(1b) Let a, b, and c be integers, and let m be an integer greater than 1. If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

TRUE FALSE

(1c) If you are told that $142 = 2 \cdot 71$ and $2^{71} \equiv 46 \pmod{143}$, then you have enough information to conclude that 143 is composite.

TRUE FALSE

(1d) The linear equation $4x - 24y = 20$ has infinitely many integer solutions.

TRUE FALSE

(1e) The Diophantine equation $x^2 + y^2 = 7$ has infinitely many integer solutions.

TRUE FALSE

(1f) The least positive residue of 22! (mod 23) is equal to 22.

TRUE FALSE

(1g) The linear congruence $18x \equiv 9 \pmod{81}$ has exactly 3 solutions in the range $\{0, \ldots, 80\}$.

TRUE FALSE

(1h) There exists an odd prime p, greater than 5, such that 2, 5, and 10 are all quadratic nonresidues of p.

TRUE FALSE

(1i) The congruence $x^2 \equiv 5 \pmod{19}$ has exactly two incongruent solutions.

TRUE FALSE

(1j) There exists an integer which has order 4 (mod 17).

TRUE FALSE

(1k) If Eve is able to compute the two prime factors of Bob's public RSA modulus, then Eve can efficiently compute Bob's private RSA key.

TRUE FALSE

(1ℓ) If $f(x)$ is a polynomial of degree n with integer coefficients, and p and q are prime numbers such that $p \neq q$, then the congruence $f(x) \equiv 0 \pmod{pq}$ has at most n^2 incongruent solutions $\pmod{pq}$.

TRUE FALSE

Problem 2: 3 parts, 15 pts total

(2a) (5 pts.) Find $\mathrm{ord}_{17}(2)$.

(2b) (5 pts.) Show that 3 is a primitive root (mod 17).

(2c) (5 pts.) Use (2b) to determine which integers in the range $\{1, \ldots, 16\}$ are quadratic residues of 17.

Problem 3: 2 parts, 16 pts total

(3a) (8 pts.) Find a complete set of incongruent solutions to $x^2 \equiv 16 \pmod{21}$.

(3b) (8 pts.) Suppose you are told the following two facts:

- $4429 = p \cdot q$, where p and q are odd prime numbers and $p \neq q$.
- There are exactly four incongruent solutions to the congruence $x^2 \equiv 1 \pmod{4429}$, and the least positive residues of those four solutions are 1, 1031, 3398, and 4428.

Find p and q.

(Hint: if $x^2 \equiv 1 \pmod{4429}$, then what do you know about the congruence class of $x^2 \pmod{p}$? What does this tell you about the congruence class of $x \pmod{p}$?)

Problem 4: 2 parts, 15 pts total

(4a) (6 pts.) Show that the number 21 is pseudoprime to the base 8.

(4b) (9 pts.) Suppose that you run the Miller-Rabin test with 3 samples to get information about the primality of the number 209, and suppose that the three random samples are 3, 33, and 116. Carry out the test. What is the conclusion?

Problem 5: 1 part, 10 pts total

Let n be a positive integer, and let a be an integer such that $(a, n) = 1$. Show that if $\{r_1, \ldots, r_{\phi(n)}\}$ is a reduced residue system (mod n), then $\{a \cdot r_1, \ldots, a \cdot r_{\phi(n)}\}$ is also a reduced residue system (mod n).

Problem 6: 3 parts, 10 pts total

(6a) (4 pts.) Let p be a prime number and let a be a positive integer not divisible by p. Show that the congruence $x^2 \equiv a \pmod{p}$ has at most 2 incongruent solutions.

(6b) (2 pts.) Suppose that p is an *odd* prime and that a is an integer not divisible by p. Show that if the congruence $x^2 \equiv a \pmod{p}$ has at least one solution, then it has two incongruent solutions.

(6c) (4 pts.) Let p and q be odd primes and assume that $p \neq q$ and that a is not divisible by either of p and q. Show that the congruence $x^2 \equiv a \pmod{pq}$ either has no solutions or has exactly 4 incongruent solutions. (You can use the previous parts of this problem in your proof.)

Problem 7: 2 parts, 10 pts total

In this problem, you will prove that there exist arbitrarily long strings of consecutive integers $\{n, n+1, \ldots, n+m\}$ such that n is divisible by 2^2, $n+1$ is divisible by 3^2, $n+2$ is divisible by 5^2, and in general $n+k$ is divisible by the square of the k^{th} odd prime. (For example, $\{548, 549, 550\}$ is such a string of length 3).

(7a) (6 pts.) Let m be a positive integer. Write down a system of $m+1$ congruences such that if n is any solution to the system, then $\{n, n+1, \ldots, n+m\}$ is a string of consecutive integers such that n is divisible by 2^2, and for each k with $1 \leq k \leq m$, the integer $n+k$ is divisible by the square of the k^{th} odd prime. You may write p_k for the k^{th} odd prime. *(Hint: if you are stuck, try to do this for $m = 2$ and see if the solution produces the string* $\{548, 549, 550\}$ *given above.)*

(7b) (4 pts.) Explain why the system of congruences you wrote down actually has a solution. (This should be a straightforward application of a theorem.)

Have a great winter break!