Math 5653. Number Theory. Spring 2014. First Midterm.
Wednesday, February 26th, 2-3:20pm

Directions: No books, notes, calculators, laptops, PDAs, cellphones, web appliances, or similar aids are allowed. All work must be your individual efforts.

- Show all your work and justify all statements that you make.
- State clearly and fully any theorem you use.
- Vague statements and hand-waving arguments will not be appreciated.
- You may assume the statement in an earlier part proven in order to do a later part.

problem	1	2	3	4	5	total	bonus	overall
points	10	10	10	10	10	40	5	45
score								

Scoring system: Exam consists of **5** problems, each of which is worth **10** points. Your regular total is the sum of the best **4** out of **5** scores (so the maximum regular total is 40). If k is the lowest of your 5 scores and $k > 5$, you will get $k-5$ bonus points (so the maximum total with the bonus is 45).

Problem 1: Consider the following system of congruences:

$$\begin{cases} x \equiv 7 \mod 24 \\ x \equiv a \mod 36 \end{cases}$$

where a is a fixed integer.

Determine for which a the system has a solution and (in case when solutions exist) find a formula for the general solution.

Problem 2: Given a prime p and a nonzero integer m, let $ord_p(m)$ denote the largest e such that $p^e \mid m$.
(a) (3 pts) Recall that a positive integer n is called a perfect square if $n = m^2$ for some $m \in \mathbb{N}$. Give a characterization of perfect squares in terms of ord_p function (for various p): a positive integer n is a perfect square if and only if ... (complete the statement, no justification is necessary)

(b) (7 pts) Let m, n be positive integers, and assume that m and n are coprime. Prove that if mn is a perfect square, then m and n must both be perfect squares. **Hint:** use (a) and basic properties of ord_p function.

Problem 3: In this problem ϕ denotes the Euler function. Find all integer solutions to the equation

$$n = 3\phi(n).$$

Make sure to prove that there are no other solutions besides the ones you found.

Problem 4:
(a) (3 pts) Let p be a prime and let $m \in \mathbb{N}$ be such that $m \equiv 1 \mod (p-1)$. Prove that $x^m \equiv x \mod p$ for all $x \in \mathbb{Z}$.

(b) (7 pts) A positive integer n is called **square-free** if there is no prime p such that $p^2 \mid n$ (equivalently, n is a product of distinct primes). Prove that n is square-free $\iff$ there exists an integer $k > 1$ (depending on n) such that

$$x^k \equiv x \mod n \qquad \text{for all } x \in \mathbb{Z}.$$

Problem 5: Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients and p a prime. Let N be the number of reduced solutions to the congruence

$$f(x) \equiv 0 \mod p^2,$$

and suppose that $N < p$. Prove that the congruence $f(x) \equiv 0 \mod p^3$ also has (precisely) N reduced solutions.

Hint: Start by considering the set of solutions to $f(x) \equiv 0 \mod p$ and analyze their possible lifts taking into account the inequality $N < p$.

Extra page 1.

Extra page 2.