Number Theory, Spring 2014. Midterm #2.
Due Wednesday, April 16th in class

Directions: Provide complete arguments (do not skip steps). State clearly and FULLY any result you are referring to. Partial credit for incorrect solutions, containing steps in the right direction, may be given. If you are unable to solve a problem (or a part of a problem), you may still use its result to solve a later part of the same problem or a later problem in the exam.

Scoring system: Exam consists of **4** problems. Each of them is worth **12** points. If s_1, s_2, s_3, s_4 are your individual scores, your total is $s_1 + s_2 + s_3 + s_4 - \min\{4, s_1, s_2, s_3, s_4\}$. Thus the maximal possible total is 44, but the score of 40 counts as 100%.

Rules: You are NOT allowed to discuss midterm problems with anyone else except me. You may ask me any questions about the problems (e.g. if the formulation is unclear), but I may only provide minor hints. You may freely use your class notes, previous homework assignments, and the class textbook by Jones and Jones. The use of other books or any online sources is not allowed.

Important note: You are allowed to use the full statement of Dirichlet's theorem on primes in arithmetic progressions (not just the special cases we proved in class/homework). **Hint:** you will need to use Dirichlet's theorem in two different problems.

1. Let p be an odd prime, and let $x \in \mathbb{Z}$ be a primitive root mod p.

(a) (2 pts) Prove that x is a primitive root mod $p^2 \iff x^{p-1} \not\equiv 1 \mod p^2$.

(b) (4 pts) Let $i \in [1, p-1]$. Use (a) and the lifting theorem to prove that x or $x + ip$ is a primitive root mod p^2. Your solution should be very short and involve very few computations – solutions imitating the proof of Theorem 6.7(b) in the book will not be accepted.

(c) (4 pts) Assume that $p \equiv 1 \mod 4$. Prove that $-x$ is also a primitive root mod p.

(d) (2 pts) Use (a), (b) and (c) to prove that if $p \equiv 1 \mod 4$, then there exists $y \in [1, p-1]$ which is a primitive root mod p^2.

2.

(a) (2 pts) Let n and d be positive integers. Let G be a finite cyclic group of order n. What is the number of solutions to the equation $g^d = e$ in G as a function of n and d? An answer is sufficient.

(b) (6 pts) Let $p_1, \ldots, p_k$ be distinct odd primes, let $n = p_1 \ldots p_k$ and define $m_i = \frac{p_i - 1}{2}$. Suppose that $m_1, \ldots, m_k$ are pairwise coprime. Prove that for every prime $p > 2$, the congruence $x^p \equiv 1 \mod n$ has at most p reduced solutions.

(c) (4 pts) Prove that for any $k \in \mathbb{N}$, there exist k primes satisfying the hypothesis of (b). **Hint:** do this inductively – assume that $p_1, \ldots, p_k$ have already been constructed and argue that another prime p_{k+1} can be added to this collection so that the properties are preserved.

3. (a) (3 pts) Let $n \in \mathbb{N}$ be odd, and suppose that the congruence $x^2 \equiv 2 \mod n$ has a solution. Prove that $n \equiv 1$ or $7 \mod 8$. **Warning:** n is not necessarily prime.

Now let q be an odd prime. As in HW#8.2, define $N = q$ if $q \equiv 1 \mod 4$ and $N = 4q$ if $q \equiv 3 \mod 4$. If $q \equiv 1 \mod 4$, define $A = Q_q$, the group of quadratic residues mod q (thought of as a subgroup of U_q) and $B = U_q \setminus A$. If $q \equiv 3 \mod 4$, define

$$A(1) = \{[x]_{4q} \in U_{4q} : x \equiv 1 \mod 4 \text{ and } [x]_q \in Q_q\},$$
$$A(2) = \{[x]_{4q} \in U_{4q} : x \equiv 3 \mod 4 \text{ and } [x]_q \notin Q_q\},$$

$A = A(1) \cup A(2)$ and $B = U_{4q} \setminus A$.

(b) (3 pts) Prove that if p is an odd prime distinct from q, then

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } [p]_N \in A \\ -1 & \text{if } [p]_N \in B \end{cases}$$

Hint: Consider separately the cases $q \equiv 1 \mod 4$ (easier case) and $q \equiv 3 \mod 4$ (harder case).

(c) (3 pts) Prove that A is a subgroup of U_N.

(d) (3 pts) Use (b) and (c) to prove that there exists an integer r such that the congruence $x^2 \equiv q \mod n$ has no solutions for any **odd** integer n satisfying $n \equiv r \mod N$. **Hint:** your argument should be similar to the one in (a) except that things will be less explicit.

4. (a) (4 pts) Let $p_1, \ldots, p_k$ be distinct primes, and let $\varepsilon_1, \ldots, \varepsilon_k$ be integers each of which is equal to ±1. Prove that there exists a prime p such that $\left(\frac{p_i}{p}\right) = \varepsilon_i$ for each i. **Hint:** your computation will be easier if you impose an additional restriction on p right away. Problem 3 is relevant here.

Given an integer n and a prime $p > n$, define $f_p(n)$ to be the number of integers in the interval $[1, n]$ which are quadratic residues mod p. Define $f(n)$ to be the smallest possible value of $f_p(n)$ as p ranges over all possible primes $> n$.
We will say that n is *square-friendly* if $f(n) \geq n/2$, that is, for every prime $p > n$, at least half of integers in $[1, n]$ are quadratic residues mod p (note that different integers may serve as quadratic residues for different p). For instance, 4 is square-friendly since $\left(\frac{1}{p}\right) = \left(\frac{4}{p}\right) = 1$ for all p, so $f(4) \geq 2$. On the other hand, 3 is not square-friendly since $\left(\frac{2}{19}\right) = \left(\frac{3}{19}\right) = -1$, so $f(3) \leq f_{19}(3) \leq 1$.

(b) (4 pts) Prove that 10 is square-friendly, that is, $f(10) \geq 5$. **Hint:** This can be proved by case-by-case analysis. If you know the value $\left(\frac{q}{p}\right)$ for every prime $q < 10$, then you know $\left(\frac{n}{p}\right)$ for all $n \leq 10$.

(c) (4 pts) Prove that 100 is not square-friendly, that is, $f(100) < 50$. If you cannot prove this, try to prove as good an upper bound for $f(100)$ as you can. **Hint:** start by listing all primes between 1 and 100 (there are 25 of them).