Number Theory, Spring 2013. Midterm #2. Due Wednesday, April 10th

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 **10** points. All problems count towards your score.

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.

1.

(a) Prove that the congruence $x^2 \equiv 2 \mod 17 \cdot 23^2$ has a solution without doing any computations (except the ones you can do in your head). You may use any theorem from the book.

(b) Now find a solution to the above congruence. Show all your computations and do not use calculators.

2.

(a) Find an integer a with the property that for any prime $p > 3$, the following holds:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 6 \\ -1 & \text{if } p \equiv 5 \mod 6 \end{cases}$$

(b) Use (a) to prove that there are infinitely many primes of the form $6n+1$. (Recall that you may use the result of (a) even if you did not solve it).

3. As usual, for an integer $n > 1$, we denote by Q_n the group of quadratic residues mod n (thought of as a subgroup of U_n).

(a) Prove that if n is a prime power, then Q_n is always cyclic. **Hint:** This can be proved essentially without computations by citing suitable results from the book.

(b) Assume that n is divisible by two different primes of the form $4m+1$. Prove that Q_n is NOT cyclic.

(c) Let $p_1 = 4n_1 + 3, \ldots, p_k = 4n_k + 3$ be distinct primes such that the numbers $2n_1+1, \ldots, 2n_k+1$ are pairwise coprime, and let $n = p_1 \ldots p_k$. Prove that Q_n is cyclic.

(d) Prove that for any $k \in \mathbb{N}$, there exist k primes satisfying the hypothesis of (c). 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).

4. Let Λ be the set of all completely multiplicative functions from $\mathbb{N}$ to $\mathbb{C}$, and let Δ be the set of all multiplicative functions $f : \mathbb{N} \to \mathbb{C}$ with the property that $f(n) = 0$ whenever n is not square-free. Recall that according to our definition, a multiplicative (or completely multiplicative) function g must satisfy $g(1) = 1$

(a) Let $h \in \Lambda$, and let $H = h^{-1}$, the Dirichlet inverse of h. Prove that $H(n) = h(n)\mu(n)$ for all n and deduce that $H \in \Delta$ (here $h(n)\mu(n)$ is the regular multiplication).

(b) Now prove that for any $f \in \Delta$, its Dirichlet inverse lies in Λ. **Hint:** First guess the formula for f^{-1} in terms of f; unlike part (a), in order to write down the formula for $f^{-1}(n)$, you need to refer to the prime factorization of n.

(c) Recall that the set M of all multiplicative functions forms a group with respect to the Dirichlet product. Note that parts (a) and (b) simply say that $\Lambda = \Delta^{-1}$, that is, Λ is precisely the set of inverses of elements of Δ (and vice versa). Now let $\langle\Delta\rangle_+$ be the set of elements of M representable as $f_1 * \ldots * f_k$ with each $f_i \in \Delta$ and $k \geq 1$ (in group-theoretic terminology, $\langle\Delta\rangle_+$ is the semigroup generated by Δ). Prove that the intersection $\langle\Delta\rangle_+ \cap \Lambda$ contains just 1 element, the function I. **Hint:** What can you say about the values of elements of $\langle\Delta\rangle_+$ and Λ on prime powers?