MATH 255: ELEMENTARY NUMBER THEORY
EXAM #2 REVIEW

Problem 1. Let p be an odd prime and $k \in \mathbb{Z}_{>0}$. Show that the congruence

$$x^2 \equiv 1 \pmod{p^k}$$

has only the solutions $x \equiv \pm 1 \pmod{p^k}$.

Problem 2. Find an integer that leaves a remainder of 9 when it is divided by 10 or 11, but that is divisible by 13.

Problem 3. What is the remainder when 18! is divided by 437?

Problem 4. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ if a, b are relatively prime positive integers.

Problem 5. Show that there is no integer $n \in \mathbb{Z}_{>0}$ such that $\phi(n) = 14$.

Problem 6. Let n be an integer with $n > 6$. Show that $\phi(n) > \sqrt{n}$.

Problem 7.

(a) Show that the arithmetic function $f(n) = (-1)^{n-1}$ is multiplicative.

(b) Let g be the arithmetic function

$$g(n) = \sum_{d|n} \mu(d) f(d).$$

Show that $g(n) = 0$ if n is not a power of 2.

Problem 8. Let n be a perfect number. Show that

$$\prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) < \frac{1}{2}.$$

Problem 9. Let

$$\sigma_k(n) = \sum_{d|n} d^k$$

be the sum of the kth powers of the divisors of n for $k \in \mathbb{Z}_{\geq 0}$. Simplify the expression

$$\sum_{d|n} \mu(d) \sigma_k(n/d).$$

Problem 10. A bank encodes a 3-digit PIN using RSA encryption with exponent $e = 835$ and modulo $n = pq = 1411 = 17 \cdot 83$. If Alice's PIN is encoded as the ciphertext 002, what is her three-digit PIN?

Problem 11. Let p be an odd prime and $n = 3^p + 1$. What is the order of 3 modulo n?

Problem 12. We quote from "The Civil Heretic" in the *New York Times Magazine*, published March 25, 2009:

> Taking problems to Dyson is something of a parlor trick. A group of scientists will be sitting around the cafeteria, and one will idly wonder if there is an integer where, if you take its last digit and move it to the front, turning, say, 112 to 211, its possible to exactly double the value. Dyson will immediately say, "Oh, that's not difficult," allow two short beats to pass and then add, "but of course the smallest such number is 18 digits long." When this happened one day at lunch, William Press remembers, "the table fell silent; nobody had the slightest idea how Freeman could have known such a fact or, even more terrifying, could have derived it in his head in about two seconds." The meal then ended with men who tend to be described with words like "brilliant," "Nobel" and "MacArthur" quietly retreating to their offices to work out what Dyson just knew.

Show that Dyson is correct—and you may take longer than two seconds!

Problem 13. Let p be the prime $p = 131 = 2 \cdot 5 \cdot 13 + 1$. Use the fact that 53 has order 5 modulo p and that 39 has order 13 to find a primitive root modulo p.

Problem 14. Show that if p is prime and $p = 2q + 1$ where q is an odd prime and a is a positive integer with $1 < a < p - 1$, then $p - a^2$ is a primitive root modulo p.

Problem 15. Show that if p is an odd prime of the form $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$, then $p \equiv 1 \pmod 4$.

Problem 16. Let p be a prime of the form $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and a an odd prime. Prove that $\left(\dfrac{a}{p}\right) = 1$.

Problem 17. Evaluate the Legendre symbol $\left(\dfrac{103}{229}\right)$.

Problem 18. For which primes p does the congruence

$$x^2 + x + 1 \equiv 0 \pmod p$$

have a solution?

Problem 19. Show that if p is prime and $p \geq 7$ then there are always two quadratic residues of p that differ by 2.