Last name _____

First name _____

LARSON—MATH 353–Homework #12
Test 2 Review

Definitions. Give a definition and an **example** for each concept.

1. *property* of an object.
2. *necessary condition*.
3. *sufficient condition*.
4. *order* of x modulo n (for $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ where $\gcd(x, n) = 1$).
5. $\phi(n)$ (for integer $n \geq 1$).
6. $\sigma(n)$ (for integer $n \geq 1$).
7. An *abundant* integer.
8. A *deficient* integer.
9. A *perfect* integer.
10. *multiplicative function* (defined on the positive integers).
11. *primitive root* (in $\mathbb{Z}/n\mathbb{Z}$, for positive integer n).
12. *quadratic residue* (in $\mathbb{Z}/n\mathbb{Z}$).

Theorems. State each theorem carefully.

13. *Chinese Remainder Theorem*.
14. *Euler's Criterion*.

Proofs.Write a careful and complete proof.

15. Prove: If p is a prime and q is a primitive root modulo p then $q^1, q^2, \ldots, q^{p-1}$ are all distinct (and therefore g is a generator for the non-zero elements in $\mathbb{Z}/p\mathbb{Z}$).

Problems.

16. What is the *open problem* we investigated this semester?

17. State any other open problem in Number Theory that was mentioned in class.

18. We proved that, if an integer p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. If an integer $n > 1$ is not prime, can $\mathbb{Z}/n\mathbb{Z}$ be a field?

19. Find a solution to this system if one exists.

$$x \equiv 4 \mod 7$$

$$x \equiv 3 \mod 11.$$

20. Find natural numbers m and n such that $\phi(mn) \neq \phi(m) \cdot \phi(n)$?

21. Argue: if p and q are distinct primes primes then $\phi(pq) = \phi(p)\phi(q)$.

22. Find $\phi(p^n)$ (for prime p and positive integer n).

23. Find all four solutions to the equation: $x^2 - 1 \equiv 0 \mod 55$.

24. List *all* the degree-2 polynomials $k[x]$ where k is the field $\mathbb{Z}/3\mathbb{Z}$.

25. Check that $f = x^3 - 1$ has exactly 3 roots where $f \in (\mathbb{Z}/7\mathbb{Z})[x]$.

26. Find all *primitive roots* in $\mathbb{Z}/11\mathbb{Z}$.

27. Find all *quadratic residues* in $\mathbb{Z}/11\mathbb{Z}$.

28. Why, in $\mathbb{Z}/p\mathbb{Z}$ with primitive root q, are the even powers of q all quadratic residues?