Last name ________________________

First name ________________________

LARSON—MATH 353–Homework #7
Test 1 Review

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

1. A *conjecture* in mathematics.
2. A *counterexample* in mathematics.
3. For $a, b \in \mathbb{Z}$, a *divides* b,
4. A *prime* integer.
5. $gcd(a, b)$ for integers a, b?
6. $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, a is *congruent to* b *modulo* n
7. $n\mathbb{Z}$?
8. $\mathbb{Z}/n\mathbb{Z}$?
9. A *complete set of residues* modulo n (for natural number n)..
10. *order* of $x \mod n$ (for $n \in \mathbb{N}$ and $x \in \mathbb{Z}$, where $\gcd(x, n) = 1$).
11. A *unit* in $\mathbb{Z}/n\mathbb{Z}$ (for integer $n \geq 2$).
12. $\phi(n)$ (for integer $n \geq 1$).

Theorems. State each theorem, and give an example.

13. *Division Algorithm.*
14. *Euclidean Algorithm.*
15. *Euclid's Lemma.*
16. *Fundamental Theorem of Arithmetic*
17. The *Cancellation* proposition for congruences.
18. *Euler's Theorem.*
19. *Wilson's Theorem.*

Proofs.

20. Prove: Every natural number $n \geq 2$ is a product of primes.

Problems.

21. Compute the greatest common divisor gcd(455,1235) by factoring.

22. Compute the greatest common divisor $\gcd(455, 1235)$ using the Euclidean Algorithm (Algorithm 1.1.13 from our text).

23. Argue: for integers a, b, k and natural number n, if $a \equiv b \mod n$ then $ak \equiv bk \mod n$.

24. Suppose a, b and n are positive integers. Prove that if $a^2 | b^2$, then $a | b$.

25. Prove that if a positive integer n is a perfect square, then n cannot be written in the form $4k + 3$ for k an integer.

26. Argue that if p is prime then every non-zero element in $\mathbb{Z}/p\mathbb{Z}$ is a unit.

27. Apply the Extended Euclidean Algorithm to find $\gcd(12, 47)$ as a linear combination of 12 and 47.

28. Apply the Extended Euclidean Algorithm to find $\gcd(12, 51)$ as a linear combination of 12 and 51.

29. Use the Extended Euclidean Algorithm to find the multiplicative inverse of $12 \mod 47$.