

Name: _____

Math 4150 – Introduction to Number Theory

Spring 2008

PRACTICE QUESTIONS FOR MIDTERM # 1

1. Use the Euclidean algorithm to compute the greatest common divisor of 108 and 228.
2. Let a, b, c be integers. State a necessary and sufficient condition for the linear diophantine equation $ax + by = c$ to have integer solutions.
3.
 - a. Use the extended Euclidean algorithm to find integers x, y such that $51x + 88y = 1$.
 - b. Find all integer solutions to $51x + 88y = 2$.
 - c. Use part (a) to solve the congruence $51x \equiv 3 \pmod{88}$.
4. Suppose that $(a, b) = 1$ and $a \mid bc$. Prove that $a \mid c$.
5. Prove that a number a is divisible by 11 if and only if the alternating sum of its base 10 digits is divisible by 11.
6. Use the method of repeated squaring to compute $2^{40} \pmod{253}$.
7.
 - a. How many solutions does the congruence $12x \equiv 8 \pmod{30}$ have?
 - b. Find all solutions modulo 30 to the congruence
$$12x \equiv 6 \pmod{30}.$$
8. In any primitive Pythagorean triple (a, b, c) , prove that exactly one of a, b, c must be a multiple of 5.
9. State and prove Fermat's Little Theorem.
10.
 - a. State Euler's generalization of Fermat's Little Theorem.
 - b. If $m = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of m , give a formula for $\phi(m)$.

- c. Evaluate $\phi(1000)$.
11. Give a numerical example which illustrates how one can use Fermat's Little Theorem to prove that an integer n is composite without actually factoring n .
 12. a. Define what it means for a positive integer n to be a *Carmichael number*.
 b. Explain how Fermat's Little Theorem can be used to prove that 561 is a Carmichael number.
 13. If a is a positive integer not divisible by 3, 5, or 7, prove that $a^{12} - 1$ is divisible by 105.
 14. A certain positive integer n leaves a remainder of 1 when divided by 7, of 2 when divided by 11, and of 3 when divided by 13. What is the smallest possibility for n ?
 15. Find all positive integers n such that $\phi(n) = 20$.
 16. How many zeroes does the (base 10 representation of the) number $100!$ end with?
 17. Show that if p is prime, then the only solutions of the congruence $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$.
 18. Prove that there are infinitely many prime numbers p congruent to 3 modulo 4.
 19. Show that 49 divides infinitely many base 10 numbers of the form $999 \dots 99$.
 20. If p and $2^p - 1$ are both prime, prove that $2^{p-1}(2^p - 1)$ is a perfect number.
 21. a. Let a be a positive integer. If $(a, 10) = 1$, prove that $a^{100} \equiv 1 \pmod{1000}$. [**Hint:** Use the Chinese Remainder Theorem.]
 b. Find the last 3 decimal digits of 7^{301} .
 22. a. Find all solutions to the congruence $x^{85} \equiv 7 \pmod{29}$.
 b. Find all solutions to the congruence $x^3 \equiv 5 \pmod{51}$.

23. Let b, k, m be integers with $(b, m) = 1$ and $(k, \phi(m)) = 1$. Prove that there is a unique solution to the congruence $x^k \equiv b \pmod{m}$.
24. a. State Korselt's criterion for Carmichael numbers.
b. Use Korselt's criterion to prove that a Carmichael number must have at least 3 distinct prime factors. [**Hint:** Use the identity $pq - 1 = (p - 1)q + q - 1 = (q - 1)p + p - 1$.]
25. a. State the Rabin-Miller test for composite numbers.
b. Explain how Rabin's theorem on the existence of many Rabin-Miller witnesses for any odd composite number n , together with the Rabin-Miller test, leads to a practical probabilistic primality test.