Math 116 Number Theory
Spring 2007

Midterm 3 Practice

Name: _____

Instructor: Travis Kelm

0 pts

1. Make sure you are able to do all of the problems Homeworks 8, 9, and 10.
2. The last couple quizzes.

Instructions. Unless otherwise indicated the letter p represents a prime and the letter m represents a positive integer.

Section 9.1: Orders and Primitive Roots

1. Find all the primitive roots of 13

2. For each divisor d of 12, find all the residues r with $1 \leq r \leq 12$ such that $\text{ord}_{13}(r) = d$

3. Find all the primes less than 20 such that 3 is a primitive root.

4. Suppose that $\text{ord}_{18}(7) = 3$. Find remainder when 7^{331} is divided by 18.

5. Suppose that $\text{ord}_m(r) = 60$. Determine $\text{ord}_m(r^{35})$.

6. How many primitive roots does 257 have?

7. Find all primitive roots of 25.

8. *True*, *False*, or *Unknown*. **You should be able to provide explanations for each True statement and counterexamples for each False statement.**

(a) _____ If r is a quadratic residue of prime p then r is not a primitive root of p.

(b) _____ If $\gcd(n, b) = 1$ then $b^{\phi(m)} \equiv 1 \pmod{m}$.

(c) _____ If b is relatively prime to m then $\text{ord}_m(b) \leq \phi(m)$.

(d) _____ If b is relatively prime to m then $\text{ord}_m(b) | \phi(m)$.

(e) _____ If b is relatively prime to m then $b^t \equiv 1 \pmod{m}$ if and only if $\text{ord}_m(b) | t$.

(f) _____ All positive integers have primitive roots.

(g) _____ If r, m are relatively prime, then $\gcd(r^i, m) = 1)$ for all $i > 0$.

(h) _____ If r is a primitive root of p and if $r^i \equiv r^j \pmod{p}$ then $i \equiv j \pmod{p-1}$.

(i) _____ If an integer has a primitive root then that primitive root is unique.

(j) _____ If r is a primitive root of m and if $t \cdot r \equiv 1 \pmod{m}$ then t is a primitive root of m.

(k) _____ If r is a primitive root of 162 then r^{49} is also a primitive root.

Section 9.2: Primitive Roots

9. (a) If $\gcd(b, 257) = 1$ then what are the possible values of $\text{ord}_{257}(b)$?

(b) How many residue classes of 257 have order 16? How many have order 25? How many have order 64?

10. *True*, *False*, or *Unknown*. **You should be able to provide explanations for each True statement and counterexamples for each False statement.**

(a) _____ If p is odd prime and r is a primitive root of p, then r^2 is a primitive root of p^2.

(b) _____ If p is an odd prime and if r is a primitive root of p^2 then r is a primitive root of p^6

Section 9.4: Index Arithmetic

11. Complete the following table:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2(n)$												

12. Find all the solutions to $4x^{11} \equiv 9 \pmod{13}$.

13. Find all the solutions to $2x^9 \equiv 11 \pmod{13}$.

14. Find all the solutions to $x^x \equiv 6 \pmod{13}$.

15. *True*, *False*, or *Unknown*. **You should be able to provide explanations for each True statement and counterexamples for each False statement.**

(a) _____ If r is a solution to $2^x \equiv 89 \pmod{101}$ then $r + 100$ is also a solution.

Section 9.5: Primality Tests

16. List all known Fermat Primes.

17. Which of the following regular n-gons are constructible using only a compass and straightedge?

(a) 14-gon

(b) 25-gon

(c) 30-gon

(d) 34-gon

(e) 771-gon

18. Find all the solutions to $2x^9 \equiv 11 \pmod{13}$.

19. Find all the solutions to $x^x \equiv 6 \pmod{13}$.

Chapter 11: Quadratic Reciprocity

20. *True*, *False*, or *Unknown*. **You should be able to provide explanations for each True statement and counterexamples for each False statement.**

(a) _____ If m, b are any integers, then $b^2 \equiv (m-b)^2 \pmod{m}$.

(b) _____ If $m > 0$ there are $\dfrac{m-1}{2}$ quadratic residues modulo m.

(c) _____ $x^2 \equiv 75 \pmod{97}$ has two incongruent solutions modulo 97.

(d) _____ $x^2 \equiv -1 \pmod{257}$ has no solutions.

(e) _____ If $p \nmid a$ then $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

(f) _____ $x^2 \equiv 85 \pmod{101}$ has no solutions.

(g) _____ $x^2 \equiv 29 \pmod{541}$ has no solutions.

(h) _____ $x^2 \equiv 101 \pmod{1987}$ has no solutions.

(i) _____ $x^2 \equiv 31706 \pmod{43789}$ has no solutions.

21. Be able to compute Legendre and Jacobi symbols.