

Name:

**MATH 506** Number Theory – **Final Exam**  
Friday May 16, 2008

---

Check that you have all four pages. Show all your work. Assume multiplicativity where appropriate.

---

1. (4 points) If  $a = 2^4 13^2 19$ ,  $b = 2^3 5^2 13$  then the prime factorization of  $(a, b) =$
2. (8 points) (a) Evaluate:  $\phi(1500) =$   
(b) The remainder when  $7^{1203}$  is divided by 1500 is \_\_\_\_\_. (Hint: Euler's Theorem!).
3. (10 points) Use induction to prove that  $6^n \equiv 5n + 1 \pmod{25}$  for all positive integers  $n$ .
4. (8 points) Prove that  $\sqrt[5]{72}$  is irrational.
5. (16 points) Find all right-angled triangles with coprime integer sides and base of given length:
  - (i) 20
  - (ii) 35.

6. (14 points) (a) If  $F(n) = \sum_{d|n} \sigma(d)$  then  $F(175) =$

(b) If  $\tau(n)^2 = \sum_{d|n} g(d)$  then  $g(5^3) =$

7. (14 points) (a) What can you say about the prime factorization of  $n$  if  $\tau(n) = 8$ ?

(b) The smallest  $n$  with  $\tau(n) = 8$  is  $n =$  \_\_\_\_\_.

(c) Find three  $n$  with  $\phi(n) = 16$ . (Bonus points if you find them all!).

8. (9 points) (a) The order of 2 mod 23 is \_\_\_\_\_.

(b) If the order of  $b$  mod  $m$  is 15 then the order of  $b^6$  mod  $m$  is \_\_\_\_\_.

9. (10 points) Use the Chinese Remainder Theorem to solve the simultaneous congruences

$$x \equiv -5 \pmod{7}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 4 \pmod{6}$$

10. (10 points) What can you say about the positive integer  $b$  if  $(b, 10) = 1$  and the decimal expansion of the rational  $1/b$  has period (exactly) three?

11. (39 points) Circle True (T) or False (F).

- T F (a) If  $a^n \not\equiv a \pmod{n}$  then  $n$  is composite.
- T F (b)  $2^{70} + 1$  is a factor of  $2^{350} + 1$ .
- T F (c) 30 and 42 form an amicable pair.
- T F (d) If  $f(n)$  is multiplicative then  $f(140) = f(14)f(10)$ .
- T F (e) If  $\{b, c, d, e\}$  is a system of reduced residues mod 5 then so is  $\{3b, 3c, 3d, 3e\}$ .
- T F (f) The system  $x \equiv 7 \pmod{10}$  and  $x \equiv 13 \pmod{25}$  has no solution.
- T F (g) The Fibonacci numbers satisfy  $f_{n+3} = f_{n+1} + f_{n+2}$ .
- T F (h)  $\underbrace{111112111112111112111112111112}_{5 \text{ times}} \equiv 6 \pmod{11}$ .
- T F (i) If  $2^3 \parallel a$  and  $2^4 \parallel b$  then  $2^9 \parallel a^3 + b^2$ .
- T F (j)  $2465 = 5 \cdot 17 \cdot 29$  is a Carmichael number.
- T F (k) If  $p$  is an odd prime then the least residue of  $(p-1)! + 2^{p-1} \pmod{p}$  is zero.
- T F (l) The linear congruence  $6x \equiv 5 \pmod{33}$  has 3 solutions mod 33.
- T F (m) If  $(a, 63) = 1$  then  $a^6 \equiv 1 \pmod{63}$ .

12. (14 points)(a) Find the continued fraction expansion of  $\sqrt{30}$ .

(b) Find the quadratic  $\alpha$  with continued fraction expansion  $\alpha = [2, 3]$ .

13. (16 points) (a) Use the Euclidean algorithm to compute the greatest common divisor  $(2517, 2370)$

(b) Find all integer solutions to the equation  $2517x - 2370y = 69$ , or explain why there are none.

(c) Solve the linear congruence  $2370x \equiv 69 \pmod{2517}$  or say why no solutions exist.

14. (12 points) (a) You have decided to do RSA cryptography with modulus  $n = 131 \cdot 163$  and encode exponent 127. Give (but don't solve) a congruence that you would use to find a decode exponent  $d$ .

(b) Find the base 2 expansion of 17 and use the successive squaring method of modular exponentiation to find the least residue of  $127^{17} \pmod{541}$ .

15. (16 points) (a) Calculate the continued fraction expansion of  $722/553$

(b) Calculate the continued fraction convergents

(c) A mechanic wants a gear ratio of approximately  $722/553$ . How many teeth should the gear wheels have, assuming that no wheel has more than fifty?