

Name:

MATH 506 Number Theory – **Final Exam**
Friday May 16, 2003

Check that that you have all four pages. Show all your work.

1. (12 points) Let $a = 2^7 5^3 7^2 13^2$, $b = 2^{10} 3^7 5^4 13^3$. Find the following:

(a) The prime factorization of (a, b)

(b) The prime factorization of $[a, b]$

(c) The value of e if $2^e \parallel a^2 b^3$

2. (4 points) What is the order of 2 modulo 17?

3. (8 points) Prove that $\sqrt[3]{12}$ is irrational.

4. (8 points) Give a proof that there are infinitely many primes.

5. (14 points) (a) Find the prime factorization of $600 =$

(b) $\tau(n)$ is the number of positive divisors: $\tau(600) =$

(c) $\sigma(n)$ is the sum of the positive divisors: $\sigma(600) =$

(d) $\phi(n)$ is the Euler phi function: $\phi(600) =$

(e) $\mu(n)$ is the Möbius function: $\mu(600) =$

6. (3 points) Give a non-trivial factor of $2^{55} - 1$. (Bonus points for two).

7. (8 points) Use induction to prove that the sum of the squares of the first n Fibonacci numbers satisfies

$$f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}.$$

8. (12 points) 1 pound \approx 0.4536 kilograms

(a) Calculate the continued fraction of 0.4536

(b) Calculate the convergents

(c) A company wants its packaging to be a whole number of pounds and approximately a whole number of kilograms. What would be sensible choices of weight between 70 and 100 pounds?

9. (6 points) Prove that if $a|b$ and $a|c$ then $a^2|7bc$.

10. (24 points) Circle True (T) or False (F).

T F (a) If $8|a^2$ then $8|a$.

T F (b) $\{1, 13, -5, -6\}$ is a reduced residue system mod 8.

T F (c) If a positive integer $n < 729$ has no divisor $1 < d \leq 23$ then n is prime.

T F (d) $n = 20$ is abundant.

T F (e) The last digit of 7^{102} is a 9.

T F (f) The equation $6x \equiv 15 \pmod{21}$ has 3 solutions mod 21.

T F (g) The Fibonacci numbers satisfy $f_{n+6} = f_{n+5} + f_{n+4}$.

T F (h) The number $\underbrace{222222222222222222222222}_{21 \text{ times}}$ is divisible by 9.

T F (i) If $\{a, b, c, d\}$ is a reduced residue system mod 5 then so is $\{3a, 3b, 3c, 3d\}$.

T F (j) If $2^{n-1} \equiv -1 \pmod{n}$ then n is composite.

T F (k) If $2^n \equiv 2 \pmod{n}$ then n is prime.

T F (l) The Euler phi function satisfies $\phi(nm) = \phi(n)\phi(m)$.

11. (6 points) Use congruences to prove that $x^2 - 5y^2 = 3$ has no integer solutions.

12. (9 points) Find all right-angled triangles with coprime integer sides and one side of length 36.

13. (10 points) (a) Use the Euclidean algorithm to compute the greatest common divisor (263,271)

(b) Solve the linear equation $263x - 271y = 5$ or explain why there are no solutions.

14. (8 points) Solve the simultaneous congruences

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

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

15. (8 points) You have chosen to do RSA cryptography with modulus $n = pq$ where $p = 7$, $q = 19$.

(a) The least common multiple $[p - 1, q - 1] =$

(b) Suppose that the encode exponent is $e = 5$. Calculate a decode exponent d .

16. (10 points) (a) Suppose that $F(n) = \sum_{d|n} d^2$. Evaluate $F(40)$.

(b) Suppose that $n^2 = \sum_{d|n} f(d)$. Evaluate $f(8)$.