

Name:

MATH 506 Number Theory – **Exam I**
Wednesday February 12, 2003

Check that that you have all three pages - note that page two is on the back of page one

1. (10 points) Find integers q and r such that $-43 = 8q + r$ with

(a) $0 \leq r \leq 8$

(b) $|r| \leq 4$.

2. (12 points) (a) Use the Euclidean algorithm to compute the greatest common divisor of 253 and 69.

(b) Write this gcd as a linear combination of 253 and 69.

3. (10 points) (a) What is the least residue of 772^5 modulo 7?

(b) Give a factor of $2^{35} - 1$.

4. (9 points) Suppose that $a \equiv 5 \pmod{7}$ and $b \equiv 3 \pmod{7}$. Use the definition of congruence to prove that $ab \equiv 1 \pmod{7}$.

5. (12 points) Decide whether the following linear Diophantine equations have any solutions. If so give the general solution, if not say why there are no solutions. No need to go through the Euclidean algorithm if there is an obvious solution.

(a) $20x - 45y = 37, \quad x, y \in \mathbb{Z}$.

(b) $5x - 3y = 7, \quad x, y \in \mathbb{Z}$.

6. (8 points) Use congruences to show that the Diophantine equation has no solutions:

$$x^2 - 4y^2 = 3, \quad x, y \in \mathbb{Z}.$$

7. (9 points) Use the definition of divisibility to prove that if $a|b$ and $a|(c - 3b)$ then $a|c$.

8. (20 points) Circle True (T) or False (F).

T F (a) $a|0$ for all non-zero integers a .

T F (b) If $a \nmid b$ and $a \nmid c$ then $a \nmid bc$.

T F (c) If $a | b$ and $a | c$ then $a | (3b - 5c)$.

T F (d) If $a | d$ and $b | d$ then $(a, b) | d$.

T F (e) If $d | a$ and $d | b$ then $d | (a, b)$.

T F (f) Any integer can be written as a linear combination of 12 and 15.

T F (g) $(13 - 6q, 6) = 1$ for any integer q .

T F (h) If ab is even then a and b are even.

T F (i) For any integer b there exist unique integers q, r with $b = 6q + r$ and $|r| \leq 3$.

T F (j) If $a \equiv c \pmod{3}$ and $b \equiv d \pmod{5}$ then $ab \equiv cd \pmod{15}$.

9. (8 points) Use congruences to show that $\frac{1}{4}(n^4 - n^2)$ is an integer for all integers n .