Name: _____   **Last 4 digits SSN:** _____

Final Exam   Number Theory, Fall 2003

You must show all relevant work for credit.

1. (16 pts) (a) Define $a \equiv b \ (mod \, m)$.

(b) Define the Euler ϕ-function (not the formula, but the **definition** of $\phi(n)$ is required).

(c) Define a perfect number.

(d) State the theorem that describes all even perfect numbers.

2. (12 pts) Prove that there are infinitely many prime numbers.

3. (15 pts) Recall the theorem describing primitive Pythagorean triples: every primitive Pythagorean triple (a, b, c) with a odd and b even is of the form

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where $s > t \geq 1$ are odd integers with no common factors.

How many primitive Pythagorean triples have $a = 5025$? Justify your answer.

4. (12 pts) Let p be a prime number. Show that the only solutions of the equation $x^2 \equiv 1 \pmod{p}$ are $x \equiv 1$ or $x \equiv -1 \pmod{p}$.

5. (15 pts) Suppose a, b, c are natural numbers.

(a) (10 pts) Prove: If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

(b) (5 pts) Is the statement in (a) still true without the assumption $\gcd(a, b) = 1$? Give an example to support your answer.

6. (15 pts) Find two numbers that add up to 1000, given that one of the numbers is a multiple of 23 and the other is a multiple of 17. How many such pairs of numbers are both positive? What are they?

7. (15 pts) (a) (5 pts) Find the continued fraction expansion of $\sqrt{10}$.

(b) (10 pts) Find the minimal solution of the Pell equation $x^2 - 10y^2 = 1$ and describe how all the other solutions of this equation are found.

8. (15 pts) (a) State the Chinese Remainder Theorem for a system of two congruences.

(b) Show that the system of congruences

$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 4 \pmod{9} \end{cases}$$

has no solution. Why doesn't this contradict the Chinese Remainder Theorem?

9. (20 pts) Let $m, n \in \mathbf{N}^*$. Denote by D_m and D_n, the sets of divisors of m and n, respectively. Similarly, denote by D_{mn} the set of divisors of mn.

(a) (6 pts) Prove that if $d \in D_m$ and $e \in D_n$, then $de \in D_{mn}$.

From part (a), the function $f : D_m \times D_n \to D_{mn}$, defined by $f((d, e)) = de$ is well defined for any m and n. In class we showed that if $gcd(m, n) = 1$, then the function f is bijective. The purpose of the rest of this exercise is to investigate this function when $gcd(m, n) \neq 1$.

(b) (7 pts) Give a concrete example to show that if $gcd(m, n) \neq 1$, the function f is no longer one-to-one.

(c) (7 pts) Show that even if $gcd(m, n) \neq 1$ the function f is still onto.

10. (25 pts) Recall that $\sigma(n)$ is the sum of all divisors of n. This problem has the purpose of leading you to discover for what kind of numbers n it may happen that $\sigma(n)$ is a prime number. (You may use freely all facts that we proved in class about the function σ.)

(a) (8 pts) Compute $\sigma(2^6)$. Compute $\sigma(5^2)$. Observe that in each case the result is a prime number. Find at least 2 other values of n such that $\sigma(n)$ is a prime number.

(b) (7 pts) After some further experimentation, if necessary, try to formulate a conjecture of the type: "If $\sigma(n)$ is prime then n must be of the form _____."

(c) (10 pts) Try to prove your conjecture from part (b).